XX Edición del Premio Protección de Datos Personales de Investigación
de la Agencia Española de Protección de Datos

PREMIO 2016

El tratamiento de los datos sanitarios en la historia clínica electrónica: Caso boliviano.

Karina Ingrid Medinaceli Díaz

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

BOLETÍN OFICIAL DEL ESTADO
MINISTERIO DE LA PRESIDENCIA
Y PARA LAS ADMINISTRACIONES TERRITORIALES

EL TRATAMIENTO DE LOS DATOS SANITARIOS EN LA HISTORIA CLÍNICA ELECTRÓNICA: CASO BOLIVIANO

EL TRATAMIENTO DE LOS DATOS SANITARIOS EN LA HISTORIA CLÍNICA ELECTRÓNICA: CASO BOLIVIANO

Karina Ingrid Medinaceli Díaz

Premio Protección de Datos Personales
de Investigación 2016
Iberoamérica

Agencia Española de Protección de Datos

Agencia Estatal Boletín Oficial del Estado
Madrid, 2017

NIPO: 786-17-046-6
ISBN: 978-84-340-2401-4

IMPRENTA NACIONAL DE LA AGENCIA ESTATAL
BOLETÍN OFICIAL DEL ESTADO
Avda. de Manoteras, 54. Madrid 28050

A los amores de mi vida:
mi padre Gilberto Medinaceli
y mi esposo Mats Brorsson

Índice

PARTE III

DESARROLLO DE LA INVESTIGACIÓN

Índice de figuras

Índice de Tablas

PRÓLOGO

La Agencia Española de Protección de Datos (AEPD) impulsa la investigación apoyando trabajos destacados, originales e inéditos que tratan sobre el derecho a la protección de datos en países iberoamericanos. En la vigésima edición de los Premios Protección de Datos de la AEPD, el jurado, compuesto por los miembros del Consejo Consultivo de esta institución, ha premiado la candidatura de Karina Ingrid Medinaceli Díaz, por su obra «El tratamiento de los datos sanitarios en la historia clínica electrónica: caso boliviano».

Los datos relativos a la salud y, en especial, aquellos que forman parte de la historia clínica no sólo conforman la llave de acceso para la asistencia sanitaria sino que constituyen un elemento de gran sensibilidad que debe ser especialmente protegido. La Agencia Española de Protección de Datos siempre ha prestado atención al tratamiento de datos de salud, constatando que la sanidad se encuentra entre las diez áreas de actividad que más reclamaciones acumulan en los últimos años. Asimismo, la Agencia ha llevado a cabo iniciativas en este ámbito, como el Plan sectorial de oficio en el sector sanitario en hospitales públicos desarrollado en 1995 o la evaluación de cumplimiento de la LOPD en hospitales públicos y privados de 2010 como consecuencia del incremento de reclamaciones de tutela de derechos y denuncias detectado en relación con las historias clínicas.

La historia clínica adquiere una especial relevancia en su dimensión electrónica, ya que permite al sanitario tener información en tiempo real de sus pacientes, mejorando la asistencia y contribuyendo a una atención más personalizada. La obra cobra especial interés al efectuar un profundo análisis de los requisitos necesarios para implantar la historia clínica electrónica desde el diseño, incluyendo un estudio sobre aspectos como la interoperabilidad, seguridad y confidencialidad de la información clínica, así como sobre los estándares normativos.

Esta obra describe de forma exhaustiva las políticas y estrategias de salud en Bolivia, la organización del sistema sanitario y las funciones de las distintas instituciones y entidades que lo integran. También incluye un análisis detallado del derecho a la protección de datos en España –en particular los principios de protección de datos

en el ámbito de la salud y los derechos ARCO por parte de los pacientes, incluidas las limitaciones a los mismos– y aborda aspectos adicionales como el papel de la autorregulación y las transferencias internacionales de datos.

El apartado relativo a la historia clínica demuestra un extenso conocimiento de la normativa española, tratando aspectos novedosos como el debate sobre la propiedad de la historia, las modalidades de acceso, las anotaciones subjetivas de los profesionales, la naturaleza jurídica del documento que lo soporta y su valor probatorio. Destaca también su análisis del uso de la historia clínica con fines judiciales analizando el principio de proporcionalidad en función de los distintos procesos y jurisdicciones.

La autora realiza un minucioso estudio sobre el estado de la e-salud en Europa y el nivel de implantación de la historia clínica electrónica en distintos países del mundo, para centrarse más adelante en el Sistema Nacional de Salud en España. Finalmente, aporta avances sobre el futuro de la tecnología en este sector, como la importancia de la autenticación, la firma electrónica o las tarjetas inteligentes, recogiendo aspectos como la gestión de riesgos o la privacidad desde el diseño.

Los constantes avances derivados del binomio salud-tecnología constituyen un reto para el sector sanitario y también para la Agencia Española de Protección de Datos, que seguirá trabajando en el desarrollo de iniciativas para fomentar el cumplimiento de la ley dentro del ámbito de actuación de su Plan Estratégico, como la actualización del Plan de inspección sectorial de oficio de sanidad que se está llevando a cabo en 2017.

Mar España Martí
Directora de la Agencia Española de Protección de Datos

RESUMEN

La presente investigación tiene tres ejes principales, el tratamiento de los datos personales en el ámbito sanitario, la historia clínica e historia clínica electrónica y la seguridad de la información.

En Bolivia, la legislación relacionada a la protección de datos personales se encuentra plasmada en la Acción de Protección de Privacidad en la Constitución Política del Estado, Decreto Supremo 28168 de Acceso a la Información del Poder Ejecutivo y Código Procesal Constitucional. En el ámbito sanitario, la Ley 3131 del Ejercicio Profesional Médico constituye el marco regulatorio del quehacer médico, reconoce como derechos del paciente la confidencialidad, secreto médico respeto a la intimidad de su paciente y a recibir información y la Resolución Ministerial que aprueba la Norma Técnica para el manejo del Expediente Clínico (Historia Clínica).

La historia clínica se puede considerar como la biografía sanitaria del paciente, la transcripción de la relación médico-paciente; tiene como finalidad principal facilitar la atención o asistencia sanitaria; comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, por lo que ostenta un valor fundamental, no sólo desde el punto de vista clínico, sino también a la hora de juzgar la actuación del profesional sanitario. La historia clínica electrónica permite que sea accesible en cualquier momento y desde cualquier lugar en que se preste asistencia; integra la información de diferentes centros e incluso sistemas, facilita ayudas para la toma de decisiones y guías de práctica clínica; es segura y confidencial porque todos los accesos a la historia deben ser registrados.

Hoy en día, las tecnologías de la información y comunicaciones (TIC) ofrecen las medidas de seguridad que requiere la legislación para el tratamiento de datos sensibles, como son los datos de salud contenidos en las historias clínicas, contando para ello con medidas de seguridad como software seguro, TIC en seguridad (back up, accesos lógico y físico, cifrado, redundancia, cortafuegos y proxies, reserva), firma electrónica, auditorías informáticas, sistema de gestión de seguridad de la información, entre otros.

Palabras clave: Datos personales. Tratamiento de datos sanitarios. Historia clínica. Expediente clínico. Historia Clínica Electrónica. Médico. Paciente. Establecimiento de salud. Tecnologías de la información y comunicaciones. Seguridad de la información.

ABSTRACT

This research has three main axes, the processing of personal data in healthcare, medical records and electronic medical records and the information security.

In Bolivia, the law concerning to the protection of personal data is enshrined in the Action for the Protection of Privacy in the State Constitution, Supreme Decree 28168 of Access to Information of the Executive and Constitutional Procedural Code. In the health sector, the Law 3131 of the Medical Professional Practice constitutes the regulatory framework to doctor's work, it recognizes the confidentiality as a patient right, medical secrecy regarding his patient privacy and to receive information and the Ministerial Resolution approving the Technical Standard for the Health Record management (Medical Records).

The Medical Record can be considered as the health patient biography, the transcript of the doctor-patient relationship; primarily it aims to facilitate care or health care; it includes all of the documents relating to healthcare processes of each patient, thus it claims a fundamental value, not only from a clinical point of view, but also in judging the performance of health professionals. The electronic medical record allows the access anytime and anywhere assistance was provided; it integrates the information from different medical centers and even systems; it provides support for decision-making and clinical practice guidelines; it is safe and confidential because all access to the record must be recorded.

Nowadays, Information Technologies and Communications (ICT) provide security measures required by the legislation for the processing of sensitive data, such as health data contained in medical records, having security measures such as secure software, ICT in security (backup, logical and physical access, encryption, redundancy, firewalls and proxies, reserve), electronic signatures, computer auditing, and system security management information, among others.

Keywords: Personal data. Processing of health data. Medical Records. Health records. Electronic Medical Record. Doctor. Patient. Health facility. Information technologies and communications. Information Security.

PARTE I

INTRODUCCIÓN

CAPÍTULO I
FUNDAMENTOS DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

La irrupción de las nuevas tecnologías en la sociedad, a través de su aplicación en ámbitos como el medio ambiente, el científico, la ingeniería o las comunicaciones, es un hecho manifiesto; el sector sanitario no ha podido sustraerse a esta realidad y ha visto renovadas muchas de sus estructuras tradicionales con las nuevas opciones traídas por la aplicación de las Tecnologías de la Información y Comunicaciones (TIC) en sectores como la gestión y la administración hospitalaria, a través de la creación de bases de datos para almacenar la información hasta ahora recopilada en archivos de difícil acceso, o posibilitando proyectos como la historia clínica electrónica.

La historia clínica electrónica permite que sea accesible en cualquier momento y desde cualquier lugar en que se preste asistencia; integra la información de diferentes centros e incluso sistemas; facilita ayudas para la toma de decisiones y guías de práctica clínica. El manejo de las tecnologías de la información y las comunicaciones por parte de los establecimientos de salud (en España centros y servicios sanitarios) debe tener presente la necesidad de preservar la confidencialidad de la información de los datos de salud, salvaguardar su integridad y facilitar, a la vez, su disponibilidad.

La investigación inicia conociendo la estructura del Sistema Nacional de Salud (SNS) de Bolivia conformado por los subsectores público, seguridad social, privado sin fines de lucro y privado con fines de lucro. Las políticas de salud en Bolivia se enmarcan en primer lugar en los derechos y obligaciones determinados por la nueva Constitución Política del Estado Plurinacional (CPE) vigente desde el año 2009. El tema de salud está elevado al rango de derecho fundamental y ampliamente desarrollado en la CPE. En ese contexto, la finalidad sectorial es contribuir al paradigma del «Vivir Bien» y a la erradicación de la pobreza e inequidad, eliminando la exclusión social y mejorando el estado de salud, a través de la consolidación del ejercicio del derecho a la salud y de

la construcción del Sistema Único de Salud Familiar Comunitaria Intercultural (SAFCI), con acceso universal sin costo en el punto de atención, priorizando la promoción de la salud, la participación y el control social, con rectoría del Ministerio de Salud.

Se realiza el estudio del régimen jurídico internacional, de la Unión Europea, de España y Bolivia para el tratamiento de los datos personales en el ámbito sanitario, calificados por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) de España, como «especialmente protegidos», haciendo que se tenga una necesaria reserva y custodia de los datos personales de los pacientes que, al incorporarse a soportes electrónicos exigen un especial deber de diligencia para evitar que puedan ser conocidos por personas ajenas al proceso asistencial o no habilitadas por la ley.

La utilización de las TIC en el ámbito de los datos sanitarios puede generar, si se separa de los criterios que lícitamente han de guiarla, atentados contra derechos fundamentales de la persona, su derecho a la intimidad y el control que ésta puede ejercer sobre sus datos personales. El Reglamento de desarrollo de la LOPD de España (Real Decreto 1720/2007) establece las medidas técnicas y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamientos, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos personales.

La Ley General de Sanidad de España no cumplía la finalidad de proteger la confidencialidad de los datos sanitarios, ni establecía una regulación específica que pudiera garantizar la intimidad del paciente frente al uso más generalizado de las TIC o frente a la intervención mayoritaria de personas, servicios e instituciones diferentes, en el seguimiento del tratamiento clínico y en el uso de la historia clínica o la documentación sanitaria; para cubrir ese vacío legal, en España se promulga la Ley Básica 41/2002 Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica, que en su exposición de motivos se refiere a la intimidad personal y a la libertad individual del usuario, garantizando la confidencialidad de la información relacionada con los servicios sanitarios que se prestan. Otros puntos positivos de esta ley son: armonizar o unificar los criterios sobre la materia después de que distintas Comunidades Autónomas hubiesen promulgado su le-

gislación particular y establecer una regulación específica sobre la historia clínica.

En relación al tratamiento de los datos personales en Bolivia, el artículo 130 de la nueva Constitución Política del Estado de Bolivia establece la Acción de Protección de Privacidad (ex-Recurso de Hábeas Data) que reconoce el derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación.

La Jurisprudencia del Tribunal Constitucional boliviano, a través de la Sentencia Constitucional 0965/2004-R de 23 de junio de 2004, establece el derecho de exclusión de la «información sensible» donde tienen su acogida los datos de salud.

La Ley 3131 del Ejercicio Profesional Médico, aprobada en fecha 8 de agosto de 2005, se constituye en el marco regulatorio del quehacer médico, cumpliendo sus tareas bajo los preceptos de sus derechos y obligaciones. La Ley reconoce como derechos del paciente la confidencialidad, secreto médico, respeto a su intimidad y recibir información adecuada. Esta ley establece como documento médico oficial la historia clínica, como el conjunto de documentos escritos e iconográficos generados durante cada proceso asistencial de la persona atendida. Asimismo, establece una definición sobre el secreto médico. La Resolución 0090/2008 aprueba la Norma Técnica para el manejo del Expediente Clínico que tiene como objeto establecer la norma y metodología con fundamentos científicos, tecnológicos, administrativos, éticos y jurídicos, para la elaboración, integración, ordenamiento, uso y archivo del Expediente clínico (Historia Clínica).

Posteriormente, se conocen las figuras relacionadas con la protección de datos personales en el ámbito sanitario como los datos médicos o de salud, historia clínica y el secreto médico, juramento hipocrático que hacen los médicos de guardar la debida confidencialidad de la información que otorga el paciente en la consulta.

La seguridad de la información clínica esta garantizada con las actuales tecnologías de la información y comunicaciones, contando para ello con medidas de seguridad como software seguro, TIC en seguridad (*back up*, accesos lógico y físico, cifrado, redundancia, cortafuegos y *proxies*, reserva), firma electrónica, auditorías informáticas, sistema de gestión de seguridad de la información, entre otros. Se presume que la aplicación de las TIC añade eficiencia y aumenta la calidad de las prestaciones pero son necesarias más evaluaciones que

aseguren este punto o pongan de manifiesto los nuevos problemas que genera su uso. La integración de información clínica exige también la estandarización e integración de sistemas y de tareas, la normalización en el léxico y la codificación; el sistema de información clínica aporta un gran valor como lugar de confluencia de los profesionales sanitarios en la asistencia (Medinaceli, 2015).

La utilización de las TIC en el ámbito sanitario ha de llevarse a cabo teniendo en cuenta las ventajas e inconvenientes de la informatización, su costo, el nuevo concepto de información integral de salud, de Historia Clínica Electrónica (HCE), de Historia de Salud Electrónica (HSE), de Sistema de Información Hospitalario (HIS).

La utilización de las TIC por parte de los establecimientos de salud debe tener presente la necesidad de preservar la confidencialidad de la información de los datos de salud, salvaguardar su integridad y facilitar, a la vez, su disponibilidad.

1.2 PLANTEAMIENTO Y JUSTIFICACIÓN DE LA INVESTIGACIÓN

El derecho a la intimidad se ve implicado de forma específica en las relaciones médico-paciente; el enfermo debe confiar en el médico, y frecuentemente le confía datos reservados que no comunicaría a otros.

El derecho a la intimidad del paciente supone la obligación del profesional sanitario de mantener en secreto cualquier información proporcionada por su paciente en el ámbito estricto de la relación médico-paciente, no pudiendo revelársela a un tercero sin su consentimiento específico, o sin que se ampare en una causa legal expresa que le exima del deber de secreto. La confidencialidad deriva del derecho a la intimidad que protege contra una serie de intromisiones no deseadas en el ámbito de la salud.

Los datos de salud se consideran como datos sensibles o especialmente protegidos de acuerdo a la legislación sobre protección de datos personales.

Hasta hace pocos años el acceso a la historia clínica y a los datos sanitarios en esa relación de beneficencia-paternalismo que el médico tenía con sus pacientes era poco común o, mejor dicho, extraordinaria. Durante muchos años la información se consideraba un privilegio

que el médico podía o no conceder a sus pacientes, pero siempre según su criterio; sin embargo, la medicina ya no puede ser un arte silencioso. El médico ha de ser consciente que informar es una exigencia del deber de beneficencia que tiene hacia sus pacientes.

En el ámbito sanitario, conviene recordar que la historia clínica, sea manual o electrónica, tiene su razón de ser en facilitar la asistencia sanitaria al ciudadano y que, por tanto, la naturaleza de la información que se incluye en la misma ha de ser acorde con el citado objetivo, debiéndose recoger exclusivamente toda la información clínica necesaria para asegurar, bajo un criterio médico, el conocimiento veraz, exacto y actualizado del estado de salud del paciente por parte de los profesionales sanitarios que le atienden.

La introducción de las tecnologías de la información y de las comunicaciones (TIC) en los establecimientos de salud (centros y servicios sanitarios) se hizo a través de equipos de diagnóstico médico y de los servicios de gestión económico-financiera, como la contabilidad o la facturación y la nomina de su personal. Más tarde se desarrollaron aplicaciones para los servicios clínico-administrativos, como la gestión de camas, la cita previa de consultas externas, o la gestión del archivo de historias clínicas; a estas aplicaciones siguieron los programas de codificación de los sistemas de clasificación de pacientes. El siguiente paso ha sido la informatización de la historia clínica, que supone introducir las TIC en el núcleo de la actividad sanitaria, como es el registro de relación entre el paciente y los médicos y demás profesionales sanitarios que le atienden.

No existe ningún impedimento legal para que la información recogida en la historia clínica se informatice, es más, la historia clínica electrónica tiene el mismo valor jurídico que la historia clínica en soporte papel. La nueva historia clínica se hace accesible en cualquier tiempo y lugar en que se preste la asistencia, integra información de diferentes sistemas y establecimientos de salud; utiliza como un instrumento más los sistemas de ayuda a la toma de decisiones y guías de práctica clínica; forma parte del sistema de información del servicio de salud; y es un poderoso instrumento de mejora de la calidad y la eficiencia del sistema sanitario.

Se presume que la aplicación de las Tecnologías de la Información y las Comunicaciones (TIC) añade eficiencia y aumenta la calidad de las prestaciones, pero son necesarias más evaluaciones que aseguren este

punto o pongan de manifiesto los nuevos problemas que genera su uso. La integración de información clínica exige también la estandarización e integración de sistemas y de tareas, la normalización en el léxico y la codificación; el sistema de información clínica aporta un gran valor como lugar de confluencia de los profesionales sanitarios en la asistencia.

La seguridad de la información clínica está garantizada con las actuales Tecnologías de la Información y Comunicaciones (TIC) contando para ello con medidas de seguridad como software seguro, TIC en seguridad (*back up*, accesos lógico y físico, cifrado, redundancia, cortafuegos y *proxies*, reserva), firma electrónica, auditorías informáticas, sistema de gestión de seguridad de la información, entre otros.

El uso de las tecnologías de la información y las comunicaciones en el ámbito de los datos sanitarios puede generar, si se separa de los criterios que lícitamente han de guiarla, atentados contra derechos fundamentales de la persona, su derecho a la intimidad y el control que ésta puede ejercer sobre sus datos personales. En la presente investigación se da a conocer que hoy en día existen medidas de seguridad que brindan las TIC que resguardan la confidencialidad en el tratamiento de los datos personales en el ámbito sanitario.

Por lo antes expuesto, queda justificado el uso las Tecnologías de la Información y las Comunicaciones en el tratamiento de datos personales en el ámbito sanitario. Para ello se estudian las ventajas y desventajas que presentan las TIC para el tratamiento de los datos de salud contenidos en las historias clínicas de los establecimientos de salud del Sistema Nacional de Salud de la ciudad de La Paz-Bolivia.

1.3 PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

La definición del problema requiere una observación más o menos estructurada. Surge del planteamiento de una serie de preguntas que nacen de la observación del área del tema que se va a estudiar y de obtener información lo más completa posible acerca de este problema, acudiendo para ello a fuentes bibliográficas, especialistas del área y todo tipo de revistas especializadas que permitan conocer si el pro-

blema elegido tiene importancia y relevancia científica, contemporánea o humanística, de esta manera se elegirán problemas significativos para la ciencia y la sociedad (López Cano, 1989).

Según lo descrito anteriormente, el problema de la presente investigación se plantea de la siguiente manera:

¿Cuál es el nivel de seguridad de la información en la actual regulación en Bolivia para el manejo de la historia clínica y la historia clínica electrónica y, el mismo brinda protección al tratamiento de los datos sanitarios y al derecho fundamental a la intimidad del paciente?

Asimismo, surgen otras interrogantes relacionadas con la investigación:

¿Es necesaria una normativa específica en Bolivia para la protección de datos personales que otorgue la seguridad jurídica que requiere el tratamiento de los datos en el ámbito sanitario?

¿Cuál es el nivel de implementación de las Tecnologías de la Información y las Comunicaciones (TIC) en los establecimientos de salud del Sistema Nacional de Salud de Bolivia?

¿Actualmente qué requisitos de seguridad de la información cumplen las historias clínicas en papel e historias clínicas electrónicas en los establecimientos de salud del Sistema Nacional de Salud de la ciudad de La Paz?

1.3.1 HIPÓTESIS

Las hipótesis desempeñan un papel fundamental en el proceso de investigación ya que sirven de puente entre la teoría y un hecho empírico. Sirve de guía al investigador sobre todo a la hora de recopilar material, datos estadísticos experimentales, etc., que permiten posteriormente, contrastarlos con la realidad (González Tirados, 2004).

Las hipótesis son enunciados de posibles soluciones a problemas que hay que contrastar, finalmente expresan y definen en forma de proposición. Son afirmaciones sujetas a confirmación. Las hipótesis forman la parte fundamental del proceso investigador y sirven de guía del mismo y de ellas pueden derivarse variables del problema, el diseño y el propio análisis e interpretación de resultados (Villabella Armengol, 2009).

Por lo que la hipótesis de la presente investigación es:

La actual regulación en materia de protección de datos y seguridad de la información en Bolivia respecto del manejo de la historia clínica y la historia clínica electrónica es muy limitada, lo cual vulnera la protección en el tratamiento de los datos sanitarios afectando al derecho fundamental a la intimidad del paciente.

1.4 OBJETIVOS DE LA INVESTIGACIÓN

Las investigaciones inician por un problema al que se debe buscar y encontrar alguna solución que se pueda definir. Los objetivos son enunciados que expresan aquello que el investigador aspira obtener una vez que haya concluido su trabajo.

Definir objetivos es tratar de establecer qué es lo que se pretende lograr y alcanzar con el trabajo de investigación. Habitualmente se formula un objetivo general referido a los propósitos más amplios del estudio y otros específicos relacionados con resultados más concretos. Los objetivos deben responder a cuál sería el propósito mediante qué y cómo se realizan (González Tirados, 2004).

El objetivo general consiste en lo que pretendemos realizar en la investigación; es decir el enunciado claro y preciso de las metas que se persiguen en la investigación a realizar. Para el logro del objetivo general la investigación debe apoyarse en la formulación de objetivos específicos.

Los objetivos específicos indican lo que se pretende realizar en cada una de las etapas de la investigación. Estos objetivos deben ser evaluados en cada paso para conocer los distintos niveles de resultados. La suma de los objetivos específicos es igual al objetivo general y por tanto los resultados esperados de la investigación. Conviene anotar que son los objetivos específicos los que se investigan y no el objetivo general, ya que éste se logra como resultado (Tamayo y Tamayo, 1996).

1.4.1 OBJETIVO GENERAL

Determinar el nivel de seguridad de la información en el manejo de la historia clínica y la historia clínica electrónica en Bolivia a objeto de proteger el tratamiento de los datos sanitarios.

1.4.2 OBJETIVOS ESPECÍFICOS

Los objetivos específicos de la investigación son:

1. Analizar la estructura, funcionamiento y limitaciones del Sistema Nacional de Salud de Bolivia.

2. Analizar la legislación sobre el tratamiento de datos personales en el ámbito sanitario de España y Bol*i*via.

3. Explicar las ventajas y desventajas que brinda la historia clínica electrónica para el tratamiento de datos sanita*r*ios.

4. Identificar las medidas de seguridad que brindan las Tecnologías de la Información y Comunicación (TIC) para el tratamiento de datos personales en el ámbito sanitario.

5. Evaluar el estado de situación de la historia clínica e historia clínica electrónica en los establecimientos de salud del Sistema Nacional de Salud de la ciudad de La *Paz*.

1.5 **METODOLOGÍA**

Para dar respuesta a la pregunta de investigación, al objetivo general, objetivos específicos e hipótesis, en la presente investigación se utiliza la técnica documental mediante la cual se extrae y recolecta información de leyes de Bolivia, España y otros países, convenios del Consejo de Europa, directivas de la Unión Europea, bibliografía académica, gubernamental, publicaciones y artículos en revistas especializadas, visita de sitios web especializados, etc.

El estudio es descriptivo-explicativo, identificando las características e interrelación entre los elementos del problema, más la comprobación y análisis de todas las variables que intervienen en la hipótesis.

El enfoque de la tesis es jurídico proyectivo en tanto que realiza una suerte de predicción sobre el futuro de un aspecto jurídico. Las predicciones surgen de premisas actualmente vigentes; asimismo es jurídico-propositivo ya que su característica es evaluar las fallas de las normas o los sistemas, en este caso un vacío jurídico, y a partir del mismo proponer posibles soluciones.

Discute consecuencias y soluciones alternas, y llega a una conclusión crítica después de evaluar los datos investigados.

El procedimiento ha consistido en seleccionar el tema para seguidamente generar preguntas sobre el mismo que guían la recolección de información significativa al desarrollar la investigación.

Como técnicas de recojo de información, se trabajó con la entrevista libre o no estructurada para desarrollar el trabajo de campo, técnica de investigaciones cualitativas que busca profundizar el fenómeno de estudio.

La entrevista es una técnica de recopilación de información mediante una conversación profesional, con la que además de adquirir información acerca de lo que se investiga, tiene importancia desde el punto de vista educativo; los resultados a lograr en la misión dependen en gran medida del nivel de comunicación entre el investigador y los participantes en la misma.

De acuerdo al fin que se persigue con la entrevista, ésta puede estar o no estructurada a través de un cuestionario previamente elaborado.

Para la presente investigación, se utilizó la entrevista no estructurada, técnica aplicada en estudios descriptivos; la ventaja que ha brindado la misma es la posibilidad de adaptación y de aplicación a toda clase de sujetos y de situaciones; se ha logrado profundizar en el tema y obtener información del mismo.

1.6 MARCO EN EL QUE SE INSERTA LA INVESTIGACIÓN

El contexto en el que sustenta la investigación es la protección de datos personales en el ámbito sanitario y la utilización de las Tecnologías de la Información y Comunicaciones (TIC) en los establecimientos de salud del Sistema Nacional de Salud de la ciudad de La Paz-Bolivia.

La base legal de España está constituida por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), el Real Decreto 1720/2007 Reglamento de desarrollo de la LOPD y la Ley Básica 41/2002 Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica. En Bolivia, la base legal está constituida por los artículos 130 y 131 Acción de Protección de Privacidad de la Constitución Política del Estado, Código Procesal Constitucional, Ley 3131 del

Ejercicio Profesional Médico, Reglamento de la Ley 3131 Decreto Supremo 28562, Resolución Ministerial 0090 que aprueba la Norma Técnica para el Expediente Clínico.

La Universidad Pontificia de Salamanca define como una línea de investigación «*Innovaciones en el desarrollo del software aplicadas a Ciencias de la Salud: Biotecnología, Biomedicina y Telemedicina*», siendo en esta línea que se acoge la investigación.

PARTE II

MARCO TEÓRICO

CAPÍTULO II
ESTRUCTURA DEL SISTEMA NACIONAL DE SALUD DE BOLIVIA

2.1 **EL SISTEMA NACIONAL DE SALUD BOLIVIANO**

2.1.1 ANTECEDENTES

Los paradigmas del desarrollo económico social y cultural establecidos en la Constitución Política del Estado Plurinacional de Bolivia y en el Plan Nacional de Desarrollo (PND), el planteamiento del PSD asume como marco de referencia el Vivir Bien y la concepción social del proceso salud enfermedad, señalando el rol de lo biológico como parte de una relación dialéctica entre fuerzas determinantes más amplias y la posibilidad de que existan fenómenos singulares en los individuos. Estos son los ejes que orientan conceptualmente las alternativas estratégicas y programáticas que han orientado la fundamentación y el repensar de las relaciones entre los diversos niveles en los que se desarrolla el proceso salud-enfermedad: promoción de la salud, prevención de la enfermedad, curación, rehabilitación, recuperación, desde la epidemiología, la salud pública y la protección social.

Por tanto, la categoría de análisis y los conceptos operacionales asumidos permiten el reconocimiento de la interconexión dialéctica entre salud y desarrollo, dando lugar al conocimiento de las diferencias en la reproducción social, en el perfil epidemiológico, en el estado de salud y en el acceso a los servicios.

En consecuencia, el marco teórico referencial está dado por el Vivir Bien, el concepto social de salud y sus determinantes, la salud como derecho fundamental, la intersectorialidad, la participación social y la interculturalidad (Ministerio de Salud y Deportes, 2010).

2.1.2 FUNDAMENTACIÓN DEL VIVIR BIEN

El Vivir Bien es un concepto milenario sustentado por las cosmovisiones de los pueblos indígenas originarios, fuertemente vinculado

a la relación armoniosa con la naturaleza y a un modo de realización humana desde una vivencia holística y comunitaria. La filosofía ancestral del Vivir Bien ha sido retomada en las políticas nacionales de desarrollo principalmente a partir del año 2006, y constituye el fundamento del Plan Nacional de Desarrollo «Bolivia Digna, Soberana, Productiva y Democrática para Vivir Bien» y mayor reconocimiento en la Constitución Política del Estado Plurinacional (artículo 8).

En el Plan Nacional de Desarrollo (PND), se resume el Vivir Bien como el acceso y disfrute de los bienes materiales y de la realización afectiva, subjetiva, intelectual y espiritual, en armonía con la naturaleza y en comunidad con los seres humanos» (Ministerio de Salud y Deportes, 2010).

En este sentido, el Vivir Bien se constituye en la base de un modelo de vida comunitario, donde prevalece el «todos nosotros» sobre el «yo», se privilegia la complementariedad, la armonía y la interdependencia, se desarrollan las condiciones materiales y al mismo tiempo las espirituales, las relaciones sociales, las redes sociales y la solidaridad; el bien común se privilegia sobre el bienestar particular, la plenitud es una condición permanente que expresa las relaciones entre las personas y el medio ambiente natural construido.

2.1.3 CONCEPTO DE SALUD

La salud no puede y no debe considerarse como un fenómeno ajeno a los procesos sociales, económicos, políticos y culturales propios de Bolivia y de su diversidad: el proceso salud/enfermedad no tiene solamente causas, sino más bien determinantes.

Esta conceptualización permite avanzar respecto a la definición que limita a la salud como «un estado de completo bienestar físico, mental y social, y no sólo la ausencia de enfermedad» (*OMS, 1946*). Por la propia condición humana, el bienestar es transitorio y difícilmente puede existir un estado de completo bienestar. Sin embargo, si se añaden parámetros para considerar las determinantes de la salud; es decir, aspectos sociales, económicos, culturales y ambientales, se puede llegar a una definición científica apegada a la realidad. En tal sentido, la propuesta en torno a la definición de salud

obliga a incorporar nuevos valores y por consiguiente, nuevas responsabilidades personales y sociales. Esto implica asumir completamente valores de igualdad, accesibilidad, gratuidad y equidad, además de armonía con la naturaleza, principios estos que privilegian la vigencia del derecho a la salud y la vida como derechos humanos y sociales fundamentales. La nueva óptica de análisis conduce a repensar la tarea del personal de salud y de las organizaciones y movimientos sociales en torno al ejercicio pleno del derecho a la salud (Cuentas, 2015).

Por tanto, al asumir la salud como un proceso multidimensional de contradicciones, entre situaciones destructivas y protectoras para la vida y la salud, que son específicas en cada espacio social, con sus características productivas, organizativas, culturales y de relaciones históricas con el medio ambiente, que se dan en momentos concretos e interdependientes de clase social, género y cultura, se la entiende como la relación de profunda armonía, complementariedad, interdependencia, solidaridad, reciprocidad, espiritualidad y equilibrio de las personas consigo mismas, con la familia, la comunidad, con todos los demás seres, con la Madre Tierra y el cosmos que nos cobija respetando, aceptando y valorando a todos con sus diferencias (Ministerio de Salud y Deportes, 2010).

2.1.4 POLÍTICAS Y OBJETIVOS DEL SISTEMA DE SALUD

Las políticas de salud en Bolivia se enmarcan en primer lugar en los derechos y obligaciones determinados por la Constitución Política del Estado Plurinacional (CPE), vigente desde el año 2009. El tema de salud está elevado al rango de derecho fundamental y ampliamente desarrollado en la Constitución (CPE, 2009). Los principales temas abordados son los siguientes:

Derecho a la vida y a la integridad física, psicológica y sexual, sin violencia (artículo 15);

La salud como un derecho fundamental (artículo 18); Determinantes sociales y salud (artículos 16, 17, 19 y 20);

Derecho a la salud de las naciones y pueblos indígenas y originarios (artículo 30);

Acceso gratuito de la población a servicios de salud (artículo 35);

Sistema Único de Salud incluyente de las medicinas tradicionales (artículo 35);

Acceso al Seguro Universal de Salud y ejercicio de los servicios (artículo 36);

Obligación del Estado a garantizar y sostener el derecho a la salud (artículo 37);

Priorización de la promoción de la salud y prevención de enfermedades (artículo 37);

Propiedad del Estado de los bienes y servicios públicos de salud (artículo 38);

Prestación ininterrumpida de los servicios de salud (artículo 38);

El Estado garantiza el servicio de salud público (artículo 39);

Reconocimiento del servicio de salud privado (artículo 39);

Vigilancia de la calidad de atención (artículo 39);

Participación de la población en la toma de decisiones y gestión del sistema (artículo 40);

Acceso a los medicamentos, priorizando los genéricos (artículo 41);

Promoción y práctica de la Medicina Tradicional (artículo 42);

Derechos de los pacientes (artículos 43 y 44);

Derecho a la Seguridad Social (artículo 45);

Derechos de los niños y prohibición de la violencia en su contra (artículos 59 a 61);

Derechos sexuales y reproductivos (artículo 66);

Derechos y protección de adultos mayores (artículo 68);

Salud integral de personas con discapacidad (artículo 70).

En alineación con la Constitución y diferentes documentos estratégicos nacionales (Plan Nacional de Desarrollo, Planes de Gobierno, etc.), el Ministerio de Salud elaboró el Plan Sectorial de Desarrollo (PSD) que determina las políticas de salud del Estado para un periodo de cinco años 2011-2015 (Ministerio de Salud y Deportes, 2010).

En este documento, se reconoce a la salud como un proceso multidimensional, estrechamente relacionado con la diversidad de procesos sociales, económicos, políticos y culturales propios a Bolivia; por lo tanto, el tema de determinantes de la salud es central en las nuevas políticas. En este contexto, la finalidad sectorial planteada es contribuir al paradigma del Vivir Bien y a la erradicación de la pobreza e inequidad, eliminando la exclusión social y mejorando el estado de salud, a través de la consolidación del ejercicio del derecho a la salud y de la construcción del Sistema Único de Salud Familiar Comunitaria Intercultural, con acceso universal sin costo en el punto de atención, priorizando la promoción de la salud, la participación y el control social, con rectoría del Ministerio de Salud. Para lograr la finalidad, se definieron tres ejes de desarrollo que orientan el accionar sectorial (Ministerio de Salud, 2010):

— *Primer Eje. «Acceso universal al Sistema Único de Salud Familiar Comunitario intercultural»:* busca efectivizar el acceso universal a servicios de salud integrales y de calidad sin costo en el punto de atención, para toda la población, en sus diferentes ciclos de vida y en igualdad de condiciones.

— *Segundo Eje. «Promoción de la Salud y Movilización Social»:* tiene como objetivo incidir en la transformación de las determinantes de la salud a partir de la participación social e intersectorial.

— *Tercer Eje. «Rectoría y Soberanía en Salud»:* tiene como objetivo recuperar y ejercer la autoridad sanitaria soberana de las instituciones que conducen y dirigen el sector en el marco de las autonomías, para asegurar el cumplimiento eficiente y efectivo de las políticas, programas y proyectos sectoriales en todo el territorio.

Finalmente, otro marco estratégico y legal clave es la Política de Salud Familiar Comunitaria Intercultural (SAFCI), que complementa y articula recíprocamente a los médicos académicos y tradicionales con la persona, familia y comunidad, Madre Tierra y cosmos vivo, en base a sus organizaciones en los ámbitos de gestión y de atención de la salud. La SAFCI tiene el objetivo principal de garantizar la inclusión y acceso universal a la salud, reconociendo que este es un derecho político, social, económico, cultural y ambiental, de todas las bolivianas y todos los bolivianos, donde los problemas de salud se

resolverán en la medida en que se tomen acciones sobre sus determinantes a partir de la corresponsabilidad de los actores en la toma de decisiones sobre la atención de salud, mediante la gestión participativa; en el marco de la reciprocidad y complementariedad con todas las medicinas.

Los cuatro principios de la Salud Familiar Comunitaria Intercultural que guían el accionar del Sector Salud son la Participación Comunitaria, la Intersectorialidad, la Interculturalidad y la Integralidad (capacidad del servicio de salud para concebir el proceso salud enfermedad como una totalidad, que contempla la persona y su relación con la familia, la comunidad, la naturaleza y el mundo espiritual; con el fin de implementar procesos de promoción de la salud, prevención y atención de la enfermedad, rehabilitación y recuperación con calidad y calidez, en el marco de los enfoques de derechos, género, generacional, étnico y otros). Si bien la Salud Familiar, Comunitaria, Intercultural es una política que se pretende implementar en todos los niveles institucionales y de atención del sector, se operativiza solo en el Sub-Sector Público y a través de algunos programas, como los médicos especialistas SAFCI, los equipos móviles SA FCI y el Programa Mi Salud, entre otros (Ministerio de Salud y Deportes, 2010).

2.1.5 LA PARTICIPACIÓN SOCIAL EN SALUD

La Participación social es un proceso social por el cual un grupo de personas con problemas y necesidades de vida compartidas en un área geográfica determinada, identifican sus necesidades, toman decisiones y establecen mecanismos de solución.

A partir de la Declaración de Alma-Atá en 1978, la participación comunitaria y social se constituyó en una estrategia principal para alcanzar el propósito de «Salud para todos en el año 2000». Dentro de esta estrategia se determinó que la participación comunitaria es la clave para hacer llegar los servicios de salud a toda la población, en particular a los grupos de mayor riesgo y con menor posibilidad de acceso a ese tipo de servicio (OMS, 1990).

La participación social en salud es el derecho y el deber que tiene la población organizada para participar directamente en la toma de

decisiones de manera efectiva sobre el quehacer en salud en todos los niveles de gestión y atención, para consolidar una visión integral colectiva y no solo sectorial o corporativa. Se constituye en un factor clave para lograr el desarrollo de acciones en salud de manera corresponsable, legitimando las intervenciones sectoriales.

2.1.6 LA INTERCULTURALIDAD EN SALUD

Uno de los aspectos fundamentales del paradigma de la transformación del Estado boliviano, que cuestiona profundamente al sistema capitalista y que tiene como meta eliminar las desigualdades en los intercambios culturales y la distribución inequitativa de recursos, es la interculturalidad que se entiende como la interrelación, la interacción, la reciprocidad, la aceptación, la cohesión, la convivencia, el aprendizaje, la enseñanza, la participación, el encuentro y el diálogo entre las culturas en igualdad de condiciones.

La política de Salud Familiar Comunitaria Intercultural (SAFCI) define la interculturalidad como la complementariedad y reciprocidad entre las personas, familias y comunidades, urbano rurales, naciones y pueblos indígena originario campesinos, comunidades interculturales y afrobolivianas con las mismas posibilidades de ejercer sus sentires, saberes/conocimientos y prácticas, para reconocerse y enriquecerse; promoviendo una interacción armónica, horizontal y equitativa con la finalidad de obtener relaciones simétricas de poder, en la atención y toma de decisiones en salud.

La aplicación del principio de Interculturalidad en la política sanitaria Familiar Comunitaria Intercultural está orientada, entre otros, a eliminar la barrera cultural en el acceso a la atención de salud y a promover la participación social efectiva en la toma de decisiones (Ministerio de Salud y Deportes, 2010).

2.1.7 LA SALUD EN EL PLAN NACIONAL DE DESARROLLO

El Plan Nacional de Desarrollo *«Bolivia Digna, Soberana, Productiva y Democrática para Vivir Bien»* tiene como objetivo construir un

modelo social, económico y estatal basado en la diversidad y en lo plurinacional, articulado a través de cuatro estrategias.

— *Estrategia económica:* Bolivia Productiva, basada en los sectores que conforman la matriz productiva y los que coadyuvan a su funcionamiento.

— *Estrategia socio-comunitaria:* Bolivia Digna, incluye los sectores distribuidores de factores y medios de producción y servicios sociales.

— *Estrategia de relacionamiento internacional:* Bolivia Soberana, comprende las relaciones económicas, políticas y culturales e incluye a los sectores vinculados con el comercio e intercambio de bienes, servicios y capitales.

— *Estrategia del poder social:* Bolivia Democrática, comprende a los sectores que promueven el poder social territorializado.

La estrategia Bolivia Digna, a la cual contribuye el sector salud, plantea la erradicación de la pobreza y de la exclusión social, eliminación de la discriminación, marginación y explotación, a partir de la provisión de servicios básicos (salud, educación, agua, etc.), como también acciones que generen capacidades económicas a familias y comunidades, buscando en las sociedades sus raíces culturales, el respeto a los derechos humanos, el sentido de pertenencia, la seguridad, el respeto a las formas de organización social y los derechos de las minorías, el principio de libertad cultural y de respeto a la diferencia y a la diversidad.

Este planteamiento asume la salud como un producto del desarrollo humano, que reorienta, redimensiona y humaniza el progreso social y en el cual las determinantes de salud (educación, saneamiento, vivienda, alimentación, medio ambiente, etc.) tienen una importancia fundamental.

2.1.8 ORGANIZACIÓN DEL SISTEMA DE SALUD BOLIVIANO

El sistema de salud boliviano tiene tres características principales, la primera y la principal muestra un sistema segmentado, una segunda característica es que el sistema es muy fragmentado y la tercera es

que el mismo tiene procesos muy débiles en el ámbito regulatorio y de rectoría.

La segmentación del Sistema Nacional de Salud se da debido a que el mismo tiene tres subsectores de salud que responden a distintas formas de financiamiento, de organización, de prestaciones y que atienden a diferentes segmentos de la población: el subsector público, el subsector de la seguridad social y el subsector privado.

El subsector público, encabezado por el Ministerio de Salud, está compuesto por el conjunto de instituciones, recursos y servicios de salud dependientes de las entidades territoriales del Estado Plurinacional (Gobiernos Municipales y Departamentales), de la administración central y descentralizada. Por otra parte, existen establecimientos de salud dependientes de las Fuerzas Armadas, Policía y de las Universidades Públicas que se consideran generalmente como pertenecientes al subsector público. El subsector público está financiado principalmente por recursos provenientes de la fiscalidad general, así que por recursos provenientes de la venta de servicios y recursos externos. El subsector de la seguridad social está compuesto por diferentes entidades estatales (como la Caja Nacional de Salud) o privadas (Caja Bancaria Privada) y es regulado por el Código de Seguridad Social (aprobado por el Honorable Congreso Nacional en 1956). Su financiamiento proviene principalmente de los aportes de empleadores públicos y privados.

El subsector privado incluye los consultorios particulares, policonsultorios y clínicas con fines de lucro, además de proveedores sin fines de lucro de ONG e Iglesia. El financiamiento del subsector privado proviene principalmente de los pagos de bolsillo realizados por la población atendida, además de compra de servicios por parte de seguros privados, financiados por cotizaciones de empleadores privados o por cotizaciones individuales (Aponte, 2014).

Las políticas públicas en Bolivia también consideran un subsector de la medicina tradicional; este subsector se destaca por la forma de atención y los conocimientos utilizados (en oposición a la medicina académica), pero no por el modo de financiamiento u organización: desde este enfoque, la casi-totalidad de los proveedores de medicina tradicional y natural pertenecen al subsector privado.

Las coberturas de los subsectores son muy diferentes: así, el sector público cubre teóricamente a toda la población, ya que no restringe el

acceso a sus establecimientos. Sin embargo, la atención gratuita de los esquemas de seguros públicos (Ley 475) está reservada a la población no asegurada. En segundo lugar, el subsector de la seguridad social cubre solo a sus afiliados (aunque se estima que la mitad de los beneficiarios de la seguridad social no utilizan los servicios de este subsector): a partir de la promulgación del Código de Seguridad Social en el año 1956 y de su Reglamentación en el año 1959, la cobertura es obligatoria para todas las personas nacionales o extranjeras, de ambos sexos, que trabajan en el territorio nacional y prestan servicios remunerados mediante designación, contrato de trabajo, o contrato de aprendizaje, sean éstas de carácter privado o público.

Los principales excluidos a la sujeción del Código son los trabajadores independientes y desocupados. Cabe señalar que el trabajador(a) formal afiliado a la seguridad social de corto plazo también puede hacer beneficiar su familia (cónyuge, hijos/as) de las prestaciones de la seguridad social. El subsector privado con fines de lucro se dirige principalmente a la población con capacidad de pago para realizar gastos de bolsillo o contratar seguros privados, casi exclusivamente en áreas urbanas. Por lo tanto, el subsector público representa generalmente la única alternativa posible en los segmentos más pobres de la población para recibir una atención institucional.

La fragmentación del sistema se debe a que cada subsistema tiene sus propias infraestructuras y sus propias condiciones de acceso y atención, además de que dentro de cada subsistema, existen condiciones de acceso, costos y atención muy heterogéneas. La fragmentación impide ofrecer a la población una atención en iguales condiciones de cantidad y calidad en todo el sistema de salud boliviano. El grado de fragmentación en el sistema de salud es muy alto, con la intervención de numerosos agentes de salud que operan en forma totalmente desintegrada, tanto entre los diferentes subsectores como al interior de los mismos (por ejemplo, existe una multiplicidad de cajas de seguridad social con gasto per cápita muy heterogéneo), contribuyendo así a una repartición de los recursos inequitativa e ineficiente, a la inequidad en el acceso a servicios de salud, a la duplicación de infraestructura en algunas regiones (y carencia de la misma en otras), a los precios excesivos y diferenciados según proveedores, a la generación de distorsiones en el mercado laboral con sueldos diferenciados, a la contratación del mismo personal médico en diferentes instituciones y a la respuesta desarticulada en casos de emergencias epidemiológicas.

Finalmente, la tercera característica del sistema de salud boliviano muestra una debilidad de los procesos regulatorios y de rectoría, que comprende la incapacidad del Ministerio de Salud a regular el sistema (por lo cual se ha vuelto ejecutante de proyectos en lugar de Ente Rector), la gestión ineficaz e ineficiente del sistema de salud en todos los niveles institucionales y la insuficiencia y contradicción interna del marco jurídico en salud, que no se adecua a las prioridades del sector (Ministerio de Salud, 2010).

2.1.9 ACTORES INSTITUCIONALES Y EL ROL QUE DESEMPEÑAN EN EL SISTEMA DE SALUD BOLIVIANO

El sistema de salud boliviano segmentado y fragmentado está integrado por una multiplicidad de actores con naturaleza, características y roles muy diferentes. A continuación, se describen las características y principales roles de los diferentes actores institucionales del Sistema Nacional de Salud, precisando si estos son de naturaleza pública o privada, con o sin fines de lucro.

2.1.9.1 **Órgano Ejecutivo**

El Órgano Ejecutivo está conformado por la Presidencia del Estado Plurinacional, la Vicepresidencia y los diferentes Ministerios; encargado, a través de sus diferentes niveles de la administración central del Estado Plurinacional, de hacer cumplir la Constitución y las leyes, proponer y dirigir las políticas de gobierno y de Estado, entre otros.

Los principales ministerios que intervienen en el sistema de salud son el Ministerio de Salud (ente rector del Sistema Nacional de Salud), pero también el Ministerio de Economía y Finanzas Públicas-MEFP (encargado de distribuir los recursos del Tesoro General de la Nación a los diferentes actores públicos del sistema de salud), el Ministerio de Planificación del Desarrollo-MPD (a través de los planes de desarrollo y proyectos de inversión pública) y el Ministerio de Gobierno (administrador de establecimientos de salud de la policía).

2.1.9.2 **Ministerio de Salud**

Ministerio del Órgano Ejecutivo del Estado Plurinacional de Bolivia; máxima autoridad en salud en el país; encargado de regular, planificar, controlar y conducir el Sistema Nacional de Salud, entre otros. También ejecuta programas de salud que benefician directamente a la población (Mi Salud, Bono Juana Azurduy, programas epidemiológicos, etc.).

2.1.9.3 **Gobiernos Departamentales**

Gobiernos territoriales autónomos conformados por una asamblea departamental y un órgano ejecutivo departamental; encargados de impulsar el desarrollo económico, productivo y social a nivel departamental, y de ejercer competencias normativas, administrativas, fiscalizadoras y ejecutivas a nivel departamental, entre otros. Los Servicios Departamentales de Salud (SEDES)[1] constituyen la principal entidad sanitaria del órgano ejecutivo departamental, encargados de la rectoría en salud en el ámbito departamental, de la administración de los recursos humanos del subsector público y de la administración y funcionamiento de establecimientos de salud de tercer nivel, entre otros (SEDES, 2015).

2.1.9.4 **Gobiernos Municipales**

Gobiernos territoriales autónomos conformados por un Consejo Municipal y un Órgano Ejecutivo Municipal están encargados de impulsar el desarrollo económico local a través de la prestación de servicios públicos a la población, y de ejercer competencias normativas, administrativas, fiscalizadoras y ejecutivas a nivel municipal, entre otros. El Órgano Ejecutivo Municipal comprende generalmente una Dirección Municipal de Salud que se encarga, entre otros, de la implementación de las políticas de salud a nivel local, financiamiento de los «seguros públicos de salud» y administración/ funcionamiento de los establecimientos de salud de primer y segundo nivel.

---

[1] Por Decreto Supremo 25060 de fecha 2 de junio de 2008 pasa a denominarse Servicio Departamental de Salud (SEDES).

2.1.9.5 Instituciones Públicas Gobiernos Municipales

Son instituciones bajo tuición del Órgano Ejecutivo que tienen competencias muy específicas y especializadas. Las instituciones descentralizadas que intervienen generalmente en el sistema de salud son el Instituto Boliviano de la Ceguera (IBC), el Comité Nacional de la Persona con Discapacidad (CONALPEDIS), la Lotería Nacional de Beneficencia y Salubridad (LONABOL) (que transfiere sus beneficios al sector salud), la Central de Abastecimiento y Suministros de Salud (CEASS) y el Instituto Nacional de Salud Ocupacional (INSO), el Fondo Nacional de Inversión Productiva y Social (FPS) (que ejecuta proyectos de inversión), y la Autoridad de Fiscalización y Control de Pensiones y Seguros (APS) (que fiscaliza y controla el mercado de seguros privados) (Aponte, 2014).

2.1.9.6 Entes gestores estatales de seguridad social de corto plazo

Instituciones descentralizadas bajo tuición del Ministerio de Salud (excepto la Corporación del Seguro Social Militar, bajo tuición del Ministerio de Defensa) regidas por el Código de Seguridad Social, están encargadas de proteger y cubrir con sus servicios a sus afiliados. Las quince (15) instituciones estatales de seguridad social son la Caja Nacional de Salud (CNS), la Caja Petrolera de Salud (CPS), la Corporación del Seguro Social Militar (COSSMIL), la Caja Bancaria Estatal de Salud (CBES), la Caja de Salud del Servicio Nacional de Caminos y Ramas Anexas (CSSNCRA), la Caja de Salud CORDES, el Seguro Integral de Salud (SINEC) y los ocho (8) Seguros Sociales Universitarios (SSU) (uno por departamento, excepto en Pando) (Aponte, 2014).

2.1.9.7 Entes gestores privados de seguridad social de corto plazo

Instituciones de derecho privado (no son parte del Estado) regidas por el código de seguridad social; Encargados de proteger y cubrir con sus servicios a sus afiliados. Incluye la Caja de Salud de la Banca Privada (CSBP), que tiene el mismo modo de funcionamiento que los

demás entes gestores, y los Seguros Médicos Delegados (SMD), que cubren solamente al personal (y sus familiares) de determinadas empresas (Seguros Delegados de COTEL, SOBOCE, Manaco, SAGUAPAC, San Cristóbal, COBEE, etc.) (Aponte, 2014).

2.1.9.8 **Instituto Nacional de Seguros de Salud (INASES)**

Entidad Pública Desconcentrada dependiente del Ministerio de Salud, encargada de regular, evaluar y fiscalizar los entes gestores de la Seguridad Social de Corto Plazo (INASES, 2015).

2.1.9.9 **Universidades y Escuelas Técnicas**

Las universidades son instituciones descentralizadas bajo tuición del Ministerio de Educación (catorce (14) universidades públicas) o instituciones educativas de derecho privado (treinta y ocho (38) universidades privadas), encargadas de proveer educación superior y elaborar investigaciones académicas, entre otros. Las escuelas técnicas de salud son instituciones desconcentradas bajo del Ministerio de Salud (dos escuelas, en La Paz y Cochabamba) o instituciones educativas de derecho privado, encargadas principalmente de la formación de técnicos superiores (como auxiliares de enfermería). Además de la formación del personal de salud, las universidades y escuelas pueden administrar sus propios establecimientos de salud (clínicas, laboratorios, etc.) para proveer servicios a la población.

2.1.9.10 **Instituciones sin fines de lucro**

Son organizaciones, asociaciones, fundaciones u otros de derecho privado, independientes de los Gobiernos nacionales y de las Organizaciones internacionales; en el sector salud, implementan proyectos según su área de especialización (salud sexual y reproductiva, salud comunitaria, etc.) y pueden administrar establecimientos de salud, entre otros. Generalmente, se considera a las instituciones nacionales como Instituciones sin Fines de Lucro al Servicios de los Hogares (ISFLSH).

2.1.9.11 Compañías de Seguros de Salud privados

Son empresas privadas que proveen seguros de salud generales que cubren el riesgo salud, seguros de personas específicos para salud y el Seguro Obligatorio de Accidentes de Tránsito (SOAT), encargados de la afiliación y administración de dichos seguros.

2.1.9.12 Empresas

Son organizaciones económicas privadas, que producen bienes y servicios diversos (actualmente no existe empresa pública del sector salud). Incluye empresas de la industria farmacéutica y médica (que fabrican y distribuyen productos farmacéuticos para tratamientos y prevención de enfermedades, así como productos médicos duraderos) y empresas privadas de provisión de servicios de salud (clínicas, laboratorios, etc.)

2.1.9.13 Colegios profesionales en salud

Son organizaciones de derecho privado con regulación y funciones de orden público, que agrupan y regulan la práctica profesional en el sector salud; están encargados de regular la práctica profesional con funciones científicas, éticas y académicas y de defender los intereses de su cuerpo profesional, entre otros.

2.1.9.14 Establecimientos de salud

Son hospitales, centros de salud u otros tipos de proveedores de servicios, públicos o privados, son encargados de la atención de la población en el diagnóstico, tratamiento, curación, rehabilitación y prevención de enfermedades, principalmente. Son generalmente clasificados en tres niveles de atención según su capacidad resolutiva. El primer nivel tiene principalmente servicios de promoción y prevención de enfermedades, consulta ambulatoria e internación de tránsito. El segundo nivel comprende atención ambulatoria de mayor complejidad e internación hospitalaria en especialidades básicas; el tercer nivel oferta la consulta ambulatoria e internación hospitalaria de es-

pecialidad y subespecialidad; servicios complementarios de diagnóstico y tratamiento de alta tecnología y complejidad.

2.1.9.15 Agencias de cooperación bilateral y multilateral

Organizaciones internacionales, agencias nacionales de cooperación o embajadas extranjeras en Bolivia, que proveen asistencia financiera y técnica al Estado Plurinacional de Bolivia en diferentes temas.

2.1.9.16 Población en general

La población en general es beneficiaria del accionar del sector salud, pero se puede volver en actor institucional a través de las organizaciones sociales y de la estructura de participación social prevista por la política SAFCI que se organizan a través de las autoridades públicas (por ello, la participación de la población tiene también un carácter público). Sin embargo, la estructura social, que incluye autoridades locales de salud y comités locales, municipales, departamentales y nacionales, se desarrolla exclusivamente en el subsector público. A través de la estructura social, la población organizada participa en el control social, pero también en su planificación (identificación de prioridades y otros).

2.2 ORGANIZACIÓN Y COMPETENCIAS INSTITUCIONALES EN SALUD DEL ESTADO

La organización de los actores públicos del sistema de salud refleja la estructura del sector público del Estado Plurinacional de Bolivia, que se detalla en el gráfico 1 a continuación, en el cual los actores institucionales que intervienen directamente en el sector salud son identificados con colores (azules). En gris claro están las unidades institucionales del Estado que no participan directamente en el funcionamiento del sistema de salud, aunque su accionar puede condicionar el desempeño del sector (por ejemplo, el Órgano Legislativo vota leyes para el sector, las empresas públicas transfieren parte de sus beneficios al Estado, lo que permite de financiar programas y proyectos de salud, etc.).

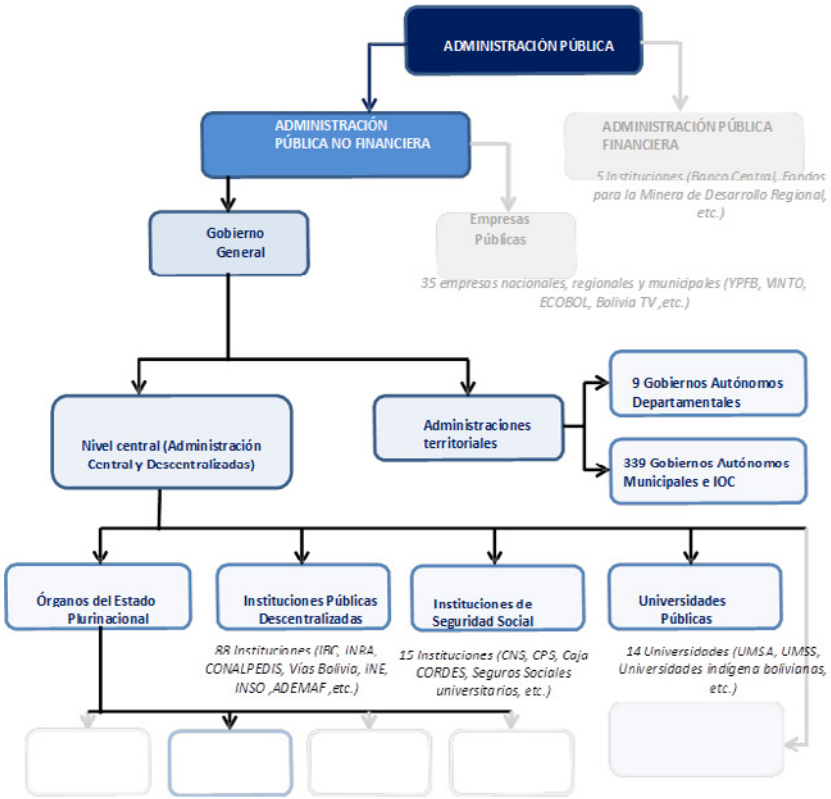

Figura 1. Estructura institucional del sector público en Bolivia en el Presupuesto General del Estado 2014

2.2.1 ORGANIZACIÓN INSTITUCIONAL

La administración pública se reparte en primer lugar entre la administración pública no financiera, que incluye la mayor parte de las entidades del estado, y la administración pública financiera, que incluye al Banco Central de Bolivia (BCB), entre otros.

La administración pública no financiera incluye a las empresas públicas por un lado y al gobierno general por otro lado. En la actualidad, no existe empresas públicas del sector salud, aunque este en discusión la creación de una fábrica pública de medicamentos; por lo

tanto, el sector salud dentro del Estado se incluye exclusivamente dentro del gobierno general. A su vez, el gobierno general se reparte entre la administración central, correspondiendo a los Órganos del Estado Plurinacional (Legislativo, Ejecutivo, Judicial y Electoral), las administraciones territoriales autónomas (gobiernos departamentales y gobiernos municipales que incluyen a las autonomías Indígena Originaria Campesinas), las 15 instituciones de seguridad social (14 Instituciones como la Caja Nacional de Salud bajo tuición del Ministerio de Salud y la Corporación del Seguro Social Militar bajo tuición del Ministerio de Defensa).

Estas categorías de instituciones son los principales agentes de financiamiento en salud del gobierno general. Adicionalmente, existen las Instituciones Públicas Descentralizadas (Agencia Boliviana de Carreteras (ABC), Insumos Bolivia, Instituto Nacional de Reforma Agraria (INRA), Instituto Nacional de Estadística (INE), Fondo Nacional de Inversión Productiva y Social (FPS), Instituto Boliviano de la Ceguera, etc.), que pueden ser especializadas en temas de salud (como por ejemplo el INSO), y las 14 Universidades Públicas. Sin embargo, las Instituciones Públicas Descentralizadas y las Universidades Públicas tienen un rol limitado en la atención en salud (Ledo y Soria, 2011).

Las principales funciones del Estado en materia de salud son desarrolladas para el subsector público de salud por el Nivel Central (principalmente el Órgano Ejecutivo a través del Ministerio de Salud) y por las Administraciones territoriales (Gobiernos Autónomos Departamentales y Municipales) y para el subsector de la seguridad social de corto plazo por las Instituciones de seguridad social. Las instituciones públicas descentralizadas y las universidades públicas solo tienen un rol secundario en el sector salud (pero las universidades tienen un rol clave en el sector educación para la formación de recursos humanos en salud).

Las competencias en materia de salud de los diferentes niveles del Estado son dictadas por la Constitución Política del Estado: el Régimen de Seguridad Social y las políticas del sistema de salud son competencias exclusivas del Nivel Central (es decir, que el nivel central tiene las facultades legislativa, reglamentaria y ejecutiva, pudiendo transferir y delegar estas dos últimas), mientras que la gestión del sistema de salud se ejerce en forma concurrente entre el nivel central (que ejerce las facultades legislativa y reglamentaria) y las entidades territoriales autó-

nomas (que ejercen la facultad ejecutiva). Asimismo, las entidades territoriales que accedan al estatuto de autonomía indígena originario campesina podrán ejercer en forma concurrente con el nivel central las competencias de organización, planificación y ejecución de políticas de salud en su jurisdicción (Ley 031). En complemento a la Constitución Política del Estado, la Ley Marco de Autonomías y Descentralización «Andrés Ibáñez» (LMAD) establece la repartición de competencias en salud entre el Nivel Central y los Gobiernos Territoriales (departamentales, municipales e indígena originario campesinas).

Por otra parte, el nivel central, que está a cargo del sistema de seguridad social como competencia exclusiva (es decir que puede delegar las facultades reglamentarias y ejecutivas), delega la atención de la seguridad social de corto plazo a 15 instituciones estatales de seguridad social públicas: la Caja Nacional de Salud (CNS), la Caja Petrolera de Salud (CPS), la Corporación del Seguro Social Militar (COSSMIL), la Caja Bancaria Estatal de Salud (CBES), la Caja de Salud del Servicio Nacional de Caminos y Ramas Anexas (CSSNCRA), la Caja de Salud CORDES, el Seguro Integral de Salud (SINEC) y los ocho Seguros Sociales Universitarios (uno por departamento, excepto en Pando). También delega la atención a instituciones privadas como la Caja de Salud de la Banca Privada y los Seguros Médicos Delegados. El sistema de seguridad social en Bolivia está vigente desde la aprobación del Código de Seguridad Social en el año 1956 y desde el año 1987, las instituciones de seguridad social se hacen cargo exclusivamente de la protección a corto plazo (enfermedad, maternidad y riesgos profesionales).

2.2.2 PRINCIPALES COMPETENCIAS

En los diferentes niveles institucionales del Estado según la Ley Marco de Autonomías y Descentralización «Andrés Ibáñez» para el sector salud se tiene las siguientes competencias:

2.2.2.1 **El nivel Central**

— Elaborar la política nacional de salud y las normas nacionales que regulen el funcionamiento de todos los sectores, ámbitos y prácticas relacionados con la salud.

— Representar y dirigir las relaciones internacionales del país en materia de salud en el marco de la política exterior y alinear y armonizar el accionar de la cooperación internacional a la política sectorial.

— Ejercer la rectoría del Sistema Único de Salud en todo el territorio y garantizar su funcionamiento mediante la implementación del Seguro Universal de Salud de acuerdo a la Ley del Sistema Único de Salud.

— Elaborar la normativa referida a la política de salud familiar comunitaria intercultural (SAFCI) y salud sexual en sus componentes de atención y gestión participativa con control social en salud.

— Promover y apoyar la implementación de las instancias de gestión participativa y control social.

— Elaborar la legislación para la organización de las redes de servicios, el sistema nacional de medicamentos y suministros y el desarrollo de recursos humanos que requiere el Sistema Único de Salud.

— Desarrollar programas de prevención de la enfermedad en territorios de alcance mayor a un departamento y gestionar el financiamiento de programas epidemiológicos nacionales y dirigir su ejecución a nivel departamental.

— Definir, coordinar, supervisar y fiscalizar la implementación de una política nacional de gestión y capacitación de recursos humanos en instituciones públicas y de la seguridad social, así que definir la política salarial, gestionar los recursos y financiar los salarios y beneficios del personal dependiente del Sistema Único de Salud.

— Coordinar con las instituciones de educación superior mediante el sistema de la Universidad Boliviana y el Ministerio de Educación, la formación de RRHH, en el marco de la política SAFCI y regular el uso de ambientes de los establecimientos de salud para la formación de RRHH por la Universidad Pública.

— Garantizar la recuperación de la medicina tradicional en el marco del Sistema Único de Salud (Parágrafo I del artículo 81 de la Ley 031).

2.2.2.2 Gobiernos Autónomos Departamentales

— Formular y aprobar el Plan Departamental de Salud en concordancia con el Plan Sectorial de Desarrollo y ejercer la rectoría en salud en el departamento, en el marco de las políticas nacionales.

— Proporcionar a establecimientos de tercer nivel la infraestructura sanitaria, el mantenimiento adecuado, servicios básicos, equipos, mobiliario, medicamentos, insumos y suministros, así como supervisar y controlar su uso.

— Planificar la estructuración de redes de salud funcionales y de calidad, en coordinación con las entidades territoriales autónomas municipales e IOC en el marco de la Política Nacional de la SAFCI.

— Establecer mecanismos de cooperación y cofinanciamiento de políticas, programas y proyectos, en coordinación con gobiernos municipales e IOC, para garantizar la provisión de servicios de salud en el departamento.

— Acreditar los servicios de salud dentro del departamento de acuerdo a la norma del nivel central del Estado.

— Ejecutar los programas epidemiológicos en coordinación con el nivel central del Estado y municipal del sector.

— Elaborar y ejecutar programas departamentales de promoción de salud y prevención de enfermedades.

— Monitorear, supervisar y evaluar el desempeño de los directores, equipo de salud, personal médico y administrativo del departamento en coordinación y concurrencia con el municipio.

— Apoyar y promover la implementación de instancias departamentales de participación y control social en salud.

— Fortalecer el desarrollo de los recursos humanos necesarios para el Sistema Único de Salud y coordinar con los municipios y universidades públicas el uso de establecimientos del Sistema de Salud para la formación de recursos humanos.

— Ejercer control en el funcionamiento y atención con calidad de todos los servicios públicos, privados, sin fines de lucro, seguridad social, y prácticas relacionadas con la salud con la aplicación de normas nacionales, así que del expendio y uso de productos farmacéuticos y otros relacionados con la salud en coordinación con municipios.

— Ejecutar las acciones de vigilancia y control sanitario del personal y poblaciones de riesgo en los establecimientos públicos y de servicios con atención a grupos poblacionales, en coordinación y concurrencia con Gobiernos Municipales (numeral 1 del parágrafo III del artículo 81 de la Ley 031).

2.2.2.3 **Gobiernos Autónomos Municipales**

— Formular y ejecutar el Plan Municipal de Salud y su incorporación en el Plan de Desarrollo Municipal.

— Implementar el Sistema Único de Salud en su jurisdicción, en el marco de sus competencias.

— Administrar la infraestructura y equipamiento y dotar a los establecimientos de primer y segundo nivel la infraestructura, el mantenimiento adecuado, servicios básicos, equipos, mobiliario, medicamentos, insumos y demás suministros, así como supervisar y controlar su uso.

— Crear la instancia máxima de gestión local de la salud a nivel municipal de acuerdo con el modelo SAFCI.

— Ejecutar el componente de atención de salud haciendo énfasis en la promoción de la salud y la prevención de la enfermedad en las comunidades urbanas y rurales.

— Ejecutar los programas nacionales de protección social en su jurisdicción territorial.

— Ejecutar acciones de vigilancia y control sanitario en establecimientos públicos y de servicios con atención a grupos poblacionales, en coordinación y concurrencia con los gobiernos departamentales (numeral 2 del parágrafo III del artículo 81 de la Ley 031).

Cabe señalar que el nivel central ejerce una multiplicidad de competencias, que se reparten entre diferentes instituciones (ministerios principalmente para la ejecución) con presupuestos propios decididos en función de los arbitrajes presupuestarios realizados por las autoridades nacionales. En cambio, con un solo presupuesto institucional, los diferentes Gobiernos autónomos departamentales y municipales deben asumir competencias en varios sectores además del sector salud: desarrollo económico y productivo, desarrollo humano, educación, energía, agua potable y saneamiento, vivienda, transporte y telecomunicaciones, medio ambiente, recursos hídricos y riego, seguridad ciudadana, ordenamiento territorial, turismo, gestión de riesgos, entre otros. Por lo tanto, según el presupuesto disponible y las prioridades políticas del Gobierno autónomo, es posible que las administraciones territoriales no asuman sus competencias en materia de salud, prefiriendo intervenir en otros sectores.

2.2.3 MINISTERIO DE SALUD

De acuerdo con la Constitución Política del Estado, según las competencias asignadas, el Ministerio de Salud tiene las siguientes atribuciones y obligaciones según el mandato político y social del Sector Salud que es el de garantizar el ejercicio pleno del derecho a la salud, la inclusión y el acceso a la salud de todas las personas, la construcción del Sistema Único de Salud en el marco de la política sanitaria de la Salud Familiar Comunitaria Intercultural, erradicando la pobreza e inequidad para el Vivir Bien.

— Formular, promulgar y evaluar el cumplimiento de los programas de salud en el marco del desarrollo del país.

— Regular, planificar, controlar y conducir el Sistema Nacional de Salud, conformado por los sectores de seguridad social a corto

plazo, público y privado con y sin fines de lucro y medicina tradicional.

— Vigilar el cumplimiento y primacía de las normas relativas a la salud pública.

— Garantizar la salud de la población a través de su promoción, prevención de las enfermedades, curación y rehabilitación.

— Ejercer la rectoría, regulación y conducción sanitaria sobre todo el sistema de salud.

— Formular, desarrollar, supervisar y evaluar la implementación del modelo de atención en salud.

— Promover la medicina tradicional y su articulación con la medicina occidental, respetando los preceptos de interculturalidad.

— Formular políticas y planes de nutrición y de seguridad alimentaria.

— Formular políticas estrategias y planes de prevención, rehabilitación y reinserción para personas farmacodependientes.

— Regular el funcionamiento de todas las entidades formadoras y capacitadoras de recursos humanos del sector salud en coordinación con el Ministerio de Educación.

— Formular políticas y ejecutar programas promoviendo la salud física y mental.

— Establecer un adecuado equilibrio de género en instancias dependientes del Ministerio.

— Establecer niveles de coordinación entre el Ministerio de Transparencia Institucional y Lucha contra la Corrupción, Viceministerio de Transparencia y Lucha contra la Corrupción, para la detección, seguimiento y sanción de casos de corrupción.

— Elaborar normas de Auditoría Médica que evalúen la calidad de la atención de las prestaciones de salud para determinar casos de «mala praxis» medica.

— Elaborar normas y reglamentos para el ejercicio de los profesionales en el área de salud.

— Formular políticas TIC, desarrollo de recursos humanos en salud; conformar el Consejo Nacional de Educación Superior en Salud, desarrollando políticas de Integración docente-asistencial.

— Promover políticas y programas de prevención, rehabilitación, capacitación y reinserción de personas con discapacidad.

— Elaborar normas de registro sanitario de medicamentos y alimentos de consumo humano.

— Elaborar normas de apertura, evaluación de servicios de salud privados: clínicas, hospitales, laboratorios, farmacias y comercializadoras de medicamentos.

— Promover convenios con instituciones formadoras de recursos humanos para el desarrollo de programas de interculturalidad y equidad de género, aplicables al área de salud.

— Promover políticas de relacionamiento, coordinación y cooperación con organismos internacionales alineados al desarrollo sectorial y a la política nacional de salud.

— Promover, elaborar e implementar la carrera profesional y sanitaria.

— Promover y patrocinar normas y reglamentos de participación social a Nivel Nacional, Departamental, Municipal y Local.

— Elaborar Normas y Reglamentos de descentralización administrativa en el marco de las autonomías Departamental Municipal y de Organizaciones Campesinas.

— Elaborar normas y reglamentar la estructura, funcionamiento y fiscalización de las instituciones públicas descentralizadas y desconcentradas.

— Promover programas conjuntos de coordinación interinstitucional con las Fuerzas Armadas y Policía Nacional, de respuesta inmediata en emergencias y desastres (artículo 90, Decreto Supremo 29894).

Por lo cual, el Ministerio de Salud ejerce la rectoría sobre el Sector Salud en el marco de las autonomías, asegurando el cumplimiento de los objetivos sectoriales en todo el territorio.

2.2.3.1 Estructura organizacional

La estructura organizacional del Ministerio de Salud es la siguiente:

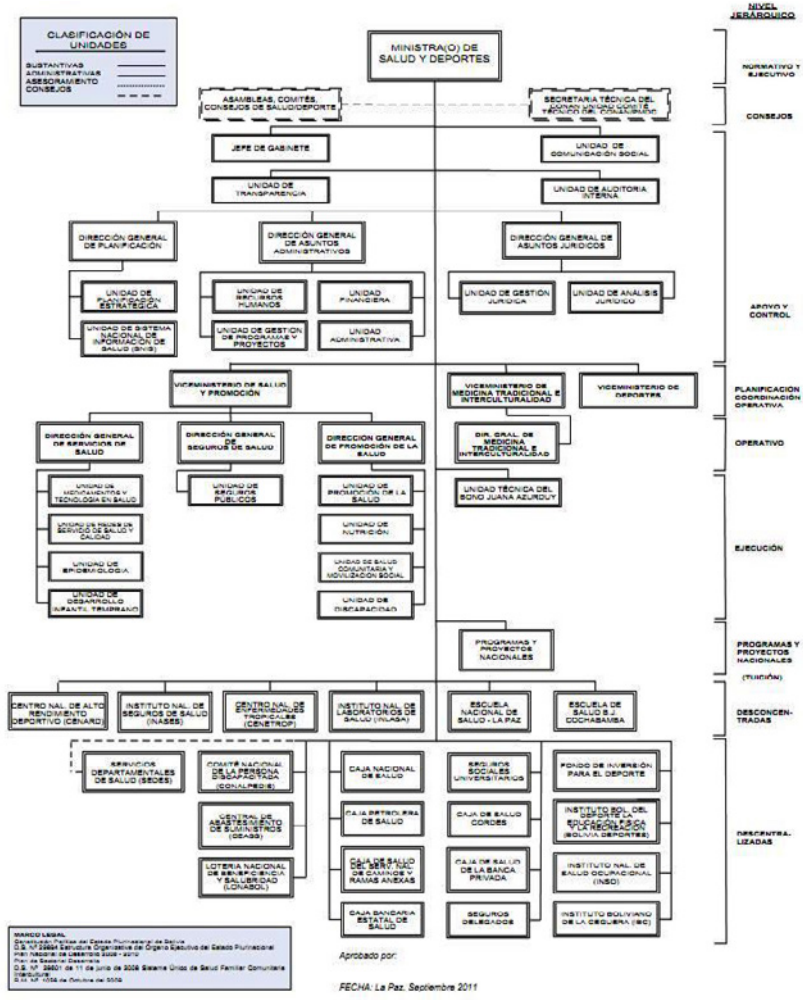

Figura 2. Estructura organizacional del Ministerio de Salud

Fuente de elaboración: Ministerio de Salud (2015).

2.2.3.2 **Plan sectorial de desarrollo**

A partir del mandato legal de la Constitución Política del Estado, del mandato estratégico del Plan Nacional de Desarrollo, del marco conceptual y del análisis situacional del sector, se establecen los siguientes ejes de desarrollo que orientarán el accionar del Sector Salud para el periodo 2010-2020 y que se operativizan dentro del Sistema Único de Salud Familiar Comunitaria Intercultural (SAFCI):

— Acceso Universal al Sistema Único de Salud Familiar Comunitario Intercultural.

— Promoción de la salud y movilización social.

— Rectoría y soberanía en salud.

Cada uno de estos Ejes de Desarrollo comprende categorías específicas de problemas:

— *Primer Eje:* Orientado a garantizar el acceso universal al Sistema Único de Salud Familiar Comunitaria Intercultural, sin costo en el punto de atención y con calidad.

— *Segundo Eje:* Orientado a incidir en las determinantes de la salud, promover el ejercicio pleno del derecho a la salud, la participación y control social en salud.

— *Tercer Eje:* Orientado a fortalecer la capacidad rectora del Ministerio de Salud y Deportes y el ejercicio de la autoridad sanitaria en todos los niveles de gestión y en todo el Sector.

Para cada Eje de Desarrollo, se incluyen Programas y Proyectos Sectoriales que contribuyen a lograr los objetivos estratégicos, el propósito y la finalidad (Ministerio de Salud y Deportes, 2010).

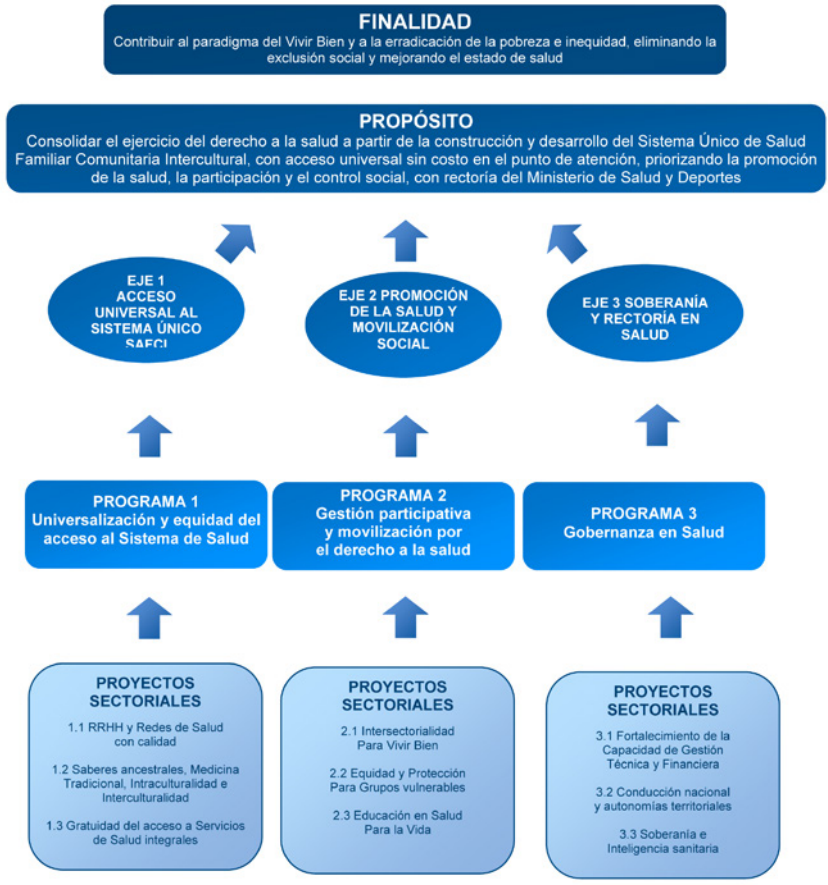

Figura 3. Plan Sectorial de Desarrollo

Fuente de elaboración: Ministerio de Salud.

2.3 POLÍTICAS Y ESTRATEGIAS DE LA POLÍTICA DE SALUD

Es en el marco de la Constitución Política del Estado, del Plan Sectorial de Desarrollo, de la política de Salud Familiar Comunitaria Intercultural (SAFCI) y de la Ley Marco de Autonomías y Descentralización, las competencias en el subsector público se desarrollan a través de la ejecución de los principales programas públicos de salud a nivel nacional, que se describen a continuación.

2.3.1 PROGRAMA DE PROTECCIÓN SOCIAL MADRE-NIÑA(O) (BONO JUANA AZURDUY)

El objetivo del programa es disminuir los niveles de mortalidad materna e infantil y la desnutrición crónica de niñas(os) menores de 2 años, actualmente el único programa público de salud orientado hacia la demanda de servicios de salud, consistiendo en la entrega de incentivos monetarios en cambio de la asistencia a controles y parto en establecimientos de salud del subsector público, se compone por:

— *Bono control prenatal:* Entrega de hasta 4 bonos (Bs. 200[2] en total) en efectivo a mujeres embarazadas condicionando a asistir a los controles prenatales correspondientes en el centro de salud asignado.

— *Bono parto institucional y control prenatal:* Entrega de un pago único (Bs. 120[3]) en efectivo a mujeres embarazadas con hijos/as menores de 2 años bajo la condición de tener un parto institucional (realizado en un centro de salud), realizar su control posparto hasta diez días después del parto y cumplir las recomendaciones médicas.

— *Bono controles integrales de salud:* Entrega de hasta 12 bonos (Bs. 1500[4] en total) bimestrales en 24 meses a mujeres embarazadas con hijos/as menores de 2 años con la condición de asistir a los controles integrales de salud en el centro de salud asignado, cumplir las recomendaciones nutricionales y calendario de vacunas, y asistencia de la madre a sesiones y actividades educativas (Decreto Supremo 066).

2.3.2. PROGRAMA MI SALUD

El objetivo del programa es fortalecer el Sistema de Salud mediante la implementación de la Salud Familiar Comunitaria Intercultural (SAFCI) y visitas domiciliarias para contribuir al paradigma del

---

2 Aproximadamente 26 euros.
3 Aproximadamente 15 euros.
4 Aproximadamente 193 euros.

Vivir Bien, el Programa Mi Salud[5] está operativizado por los médicos bolivianos egresados de la Escuela Latinoamericana de Medicina (ELAM), que se moviliza principalmente a través de visitas a comunidades y domicilios; sus principales actividades son las siguientes:

— Acciones promoción de la salud y prevención de la enfermedad.
— Desarrollo de campañas de identificación de factores de riesgo (toma de Papanicolaou, Hipertensión Arterial, Diabetes, Fluoración, Desparasitación, Problemas del Aprendizaje, etc.)
— Fomentar la autorresponsabilidad individual, familiar y comunitaria promoviendo hábitos de higiene saludables mediante charlas educativas.
— Realizar el diagnóstico precoz y la atención integral.
— Desarrollar la rehabilitación basada en la comunidad, dirigida a las personas integrantes de los grupos vulnerables.
— Visitas de seguimiento e identificación de factores de riesgo.
— Atención de la enfermedad con enfoque integral e intercultural (Ministerio de Salud, 2015).

2.3.3 PROGRAMA MULTISECTORIAL DESNUTRICIÓN CERO (PMDC)

El programa[6] contribuye a la erradicación de la desnutrición en los niños y niñas menores de 5 años, este programa interviene principalmente en 166 municipios priorizados según su índice de vulnerabilidad a la inseguridad alimentaria (Esquivel y Uzquiano, 2008). Sin embargo,

---

[5] El Programa Mi Salud desde su implementación a nivel nacional se encuentra en 267 municipios del país, con la participación de más de 1.978 médicos que han brindado atención a 3.928.159 personas a nivel nacional, con miras a la construcción e implementación del Sistema Único de Salud (SUS). Ministerio de Salud (2015): «Oruro celebra primer año de la implementación del programa Mi Salud» [en línea]: http://www.minsalud.gob.bo/645-oruro-celebra-primer-implementacion [Consulta: 19/06/2015].

[6] Mediante Resolución Ministerial N° 0442 de fecha 18 de junio de 2007 el Ministerio de Salud y Deportes aprueba el documento del Programa Multisectorial Desnutrición Cero (PMDC) e instruyó su difusión al personal del Sistema Nacional de Salud.

algunas intervenciones, como el Nutribebe se realizan en todo el país. Los principales componentes del PMDC son los siguientes:

— Atención Integral a las Enfermedades Prevalentes de la Infancia (AIEPI) con los componentes AIEPI-Nut Clínico (niño y niña menor de cinco años) y AIEPI-Nut (comunidad).

— Atención al desnutrido severo, capacitación a hospitales de segundo y tercer nivel para la atención del desnutrido severo.

— Hospital Amigo de la Madre y el Niño, certificación de los hospitales de segundo y tercer nivel en cuanto a la calidad de atención de la madre y del niño, con énfasis en la lactancia exclusiva de seis meses.

— Fortificación de alimentos para niños y niñas, elaboración y seguimiento de las fórmulas de fortificación.

— Alimento complementario «Nutribebe» dirigido a mejorar la alimentación de los niños y niñas entre seis meses y dos años.

— Micronutrientes, vitamina A y chispitas nutricionales, enfocado a niños y niñas entre los dos y cinco años de edad.

— Unidades Nutricionales Integrales (UNI), unidades de nutrición en los municipios, idealmente deberían contar con un nutricionista, una auxiliar de enfermería y una trabajadora social (Ministerio de Salud, 2015).

2.3.4 PROGRAMAS VERTICALES DE EPIDEMIOLOGÍA

El programa pretende garantizar la prevención, control y/o erradicación de enfermedades transmisibles y no transmisibles. Los programas epidemiológicos verticales dependen generalmente de la Unidad de Epidemiología del Ministerio de Salud y trabajan en coordinación con los Gobiernos territoriales. Son encargados principalmente de la compra y distribución de medicamentos e insumos para la prevención y tratamiento de enfermedades transmisibles y no transmisibles y/o otras condiciones de salud, así como de la elaboración de las estrategias nacionales de prevención y control de enfermedades. Los programas verticales nacionales incluyen los Programas nacionales de vigilancia y control de Tuberculosis; ITS/VIH/SIDA; Malaria; Dengue; Chagas; Leishmaniasis; Lepra; Cólera y Enfermedades transmitidas

por Alimentos; Hantavirus y enfermedades transmitidas por Roedores; accidentes por Ofidios y Ponzoñosos; Zoonosis y Rabia; programa nacional de vigilancia control y atención de Desastres; Programa nacional de vigilancia y atención sanitaria Influenza A/H1N1; Programa nacional de Enfermedades no Transmisibles; Programa prevención de la Salud Oral a nivel nacional; Programa nacional de Salud Renal; Programa nacional de Sangre (Llanque Laimés, 2011).

2.3.5 PROGRAMAS DE RESIDENCIA MÉDICA Y EQUIPOS MÓVILES SAFCI

El programa pretende implementar la Política de Salud Familiar Comunitaria Intercultural (SAFCI) en las comunidades y redes de salud rurales a través de la formación de Médicos Residentes en SAFCI y equipos móviles SAFCI. La Residencia Médica en Salud Familiar Comunitaria Intercultural (SAFCI) y los Equipos Móviles SAFCI son programas de operativización de la política SAFCI, impulsados por el Ministerio de Salud y ahora parcialmente asumidos por los Gobiernos autónomos territoriales (para funcionamiento de equipos móviles principalmente). Las principales actividades de ambos programas son las siguientes:

— Formación de médicos especialistas en SAFCI a través de la residencia.

— Acciones de promoción de la salud y prevención de la enfermedad en coordinación con las comunidades donde operan.

— Impulsar la gestión participativa y modelo de gestión en salud.

— Coordinación con médicos tradicionales para la atención intercultural.

— Atención de la enfermedad con enfoque integral e intercultural a través de visitas a la comunidad y domiciliarias por parte de especialistas SAFCI y equipos móviles (médico, odontólogo, enfermera, chofer).

— Educación permanente a la población en Salud Familiar Comunitaria Intercultural e identificación de determinantes de la salud (Ministerio de Salud, 2015).

2.3.6 PROGRAMAS DE CONSTRUCCIÓN Y EQUIPAMIENTO DE ESTABLECIMIENTOS DE SALUD

Con este programa se pretende fortalecer la oferta de servicios de salud a través de infraestructura y equipamiento de establecimientos de salud del subsector público. Los proyectos de construcción y equipamiento de establecimientos de salud asumidos por el Ministerio de Salud, principalmente con fondos de cooperación externa, apoyan a los Gobiernos autónomos territoriales en sus competencias de construcción, ampliación, remodelación y equipamiento de establecimientos de salud. Una gran parte de los proyectos de infraestructura y equipamiento están bajo la responsabilidad del Programa Técnico Operativo de Infraestructura y Equipamiento Médico (PTOIEM), que tiene las siguientes atribuciones:

— Ejecución de proyectos de infraestructura y equipamiento con recursos del BID (hospitales de El Alto, Potosí, Llallagua, etc.).

— Revisión de características técnicas de proyectos de infraestructura y equipamiento del Ministerio de Salud o de los Gobiernos Autónomos Territoriales y apoyo en la elaboración de nuevos proyectos.

Adicionalmente, el Ministerio de Salud maneja directamente otros proyectos que financian infraestructura y equipamiento, con recursos del Banco Mundial, Italia, Francia, Japón, Alianza GAVI, etc.

Finalmente, el programa Evo Cumple, administrado por la Unidad de Proyectos Especiales (UPRE) del Ministerio de la Presidencia, ejecuta en forma directa construcciones de establecimientos de salud, principalmente de primer nivel en todo el país.

2.4 SUPERPOSICIÓN DE COMPETENCIAS EN LA ASIGNACIÓN DE RECURSOS EN EL SUBSECTOR PÚBLICO

En los hechos, el ejercicio de las competencias de los diferentes niveles de gobierno y de los programas nacionales se desarrolla con poca coordinación entre los niveles central, departamental y municipal, resultando en una superposición de competencias en el subsector

público para la asignación de recursos humanos y físicos (insumos y capital). En efecto, el nivel central (Órgano Ejecutivo) asigna recursos humanos e insumos a través de los programas Mi Salud, de Protección Social Madre-Niña(o), programas nacionales de epidemiología, SAFCI, etc., sino con poca coordinación con el establecimiento de salud en el cual trabajan estos recursos humanos (en el caso de proveedores individuales, el personal no trabaja dentro del establecimiento de salud, pero tiene alguna relación para referencia de pacientes e información en salud).

Por otra parte, el Ministerio de Economía y Finanzas Públicas y el Ministerio Salud deciden de la asignación entre cada departamento de los recursos humanos permanentes (ítems) financiados con recursos del Tesoro General de la Nación (TGN) e HIPC. A su vez, los gobiernos departamentales deciden de la asignación de estos ítems por establecimiento de salud y son encargados de su pago con recursos del Tesoro General de la Nación. Adicionalmente, los Gobiernos departamentales pueden contratar recursos humanos con sus propios recursos y asignar recursos físicos, generalmente para establecimientos de salud de tercer nivel (que son su competencia de acuerdo con la Ley Marco de Autonomía y Descentralización); sin embargo, algunos gobiernos departamentales, como el de Tarija, pueden manejar programas departamentales que financian recursos humanos e insumos directamente a los establecimientos de salud de Nivel I, II o III o transfiriendo recursos a los gobiernos autónomos municipales.

Los Gobiernos Autónomos Municipales asignan recursos y contratan personal, principalmente para los establecimientos de salud de primer y segundo nivel. También están a cargo de la ejecución de la Ley de prestaciones de servicios de salud integral del Estado, a través de la cual financian la compra de medicamentos e insumos para la atención de la población cubierta, en los tres niveles de atención. Adicionalmente, los establecimientos de salud manejan un presupuesto propio con los ingresos generados mediante la venta de servicios a la población en general y a otras instituciones. Con este presupuesto, contratan recursos humanos, pagan servicios y compran los insumos y bienes de capital necesarios a su actividad y que no les fueron asignados por el nivel central, departamental o municipal.

Cabe señalar que en términos presupuestarios, las asignaciones con recursos propios de los establecimientos se registran dentro del presupuesto de la entidad a la cual estos pertenecen (gobiernos municipales el primer y segundo nivel, gobierno departamental para tercer nivel).

En cuanto a recursos humanos, existen entonces, a nivel local, personas que obedecen a diferentes niveles del Estado, con formas de contratación y remuneraciones diferenciadas, y entre las cuales existe una insuficiente coordinación para el trabajo en equipo e ineficiencias provocadas por la mala repartición del personal inherente a esta fragmentación de competencias; así, un mismo establecimiento de salud puede funcionar con recursos humanos TGN/HIPC (ítems nacionales, administrados por los gobiernos departamentales), recursos humanos de los diferentes programas del Ministerio de Salud, recursos humanos propios del Gobierno Autónomo Departamental, recursos humanos propios del Gobierno Autónomo Municipal y recursos humanos contratados por el mismo establecimiento de salud. Para la asignación de insumos, la situación es similar, en la cual los establecimientos de salud reciben insumos desde los diferentes niveles de gobierno, lo que incrementa inevitablemente los costos administrativos y las pérdidas. De manera general, hay poca doble asignación de medicamentos y productos farmacéuticos ya que las competencias específicas de cada programa nacional (malaria, tuberculosis, etc.) no son repetidas a nivel o local; sin embargo, cuando hay penuria o problemas logísticos en un programa nacional del nivel central, los productos farmacéuticos no son asignados por los niveles municipal y departamental (Aponte, 2014).

Finalmente, existe también una superposición de competencias para la asignación de bienes de capital (construcción o refacción de establecimientos de salud y equipamiento): de acuerdo con la LMAD, los gobiernos autónomos departamentales están encargados de la construcción y equipamiento en el tercer nivel, mientras que los gobiernos municipales están encargados del primer y segundo nivel. Pero adicionalmente, el nivel central ejecuta proyectos de construcción y equipamiento en los tres niveles de atención, a través de proyectos con financiamiento externo del Ministerio de Salud y del Programa Evo Cumple del Ministerio de la Presidencia. Si bien estos proyectos permiten la construcción y/o equipamiento de establecimientos que no hubieran necesariamente sido asumidos por los Go-

biernos departamentales y municipales (sea por falta de recursos o falta de priorización del sector salud) existe una falta de coordinación entre los diferentes niveles de gobierno, que engendra numerosos problemas al momento de abrir y hacer funcionar la infraestructura si el nivel central, los gobiernos departamentales y los gobiernos municipales no asignan el personal y los insumos necesarios a su funcionamiento.

2.5 PROGRAMA ITS-VIH/SIDA

Desde el año 1992 el Ministerio de Salud de Bolivia, con el apoyo financiero de la Agencia de los Estados Unidos para el Desarrollo Internacional[7] (USAID/Bolivia), y los Centros para el Control de Enfermedades (CDC) de los Estados Unidos de Norteamérica, implementó una estrategia de prevención dirigida a poblaciones vulnerables, con la apertura de los Centros Departamentales de Vigilancia y Referencia (CDVIR) de ITS/VIH/SIDA, iniciando este proyecto en una primera etapa en la ciudad de La Paz; posteriormente, este programa se extendió a las nueve (9) capitales de departamento en todo el País.

---

[7] La Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) es una agencia independiente que proporciona asistencia económica, de desarrollo y humanitaria alrededor del mundo apoyando las metas de la política exterior de los Estados Unidos. La agencia trabaja en 100 países en desarrollo y de manera conjunta con organizaciones privadas voluntarias, grupos indígenas, universidades, empresas estadounidenses, organizaciones internacionales, otros gobiernos, asociaciones laborales y profesionales, organizaciones fundamentadas en la fe y otras agencias del gobierno de los Estados Unidos. USAID tiene relaciones de trabajo, a través de contratos y acuerdos de donación, con más de 3.500 compañías y más de 300 organizaciones privadas de voluntariado con sede en los Estados Unidos. La cooperación técnica y económica a Bolivia data desde 1943, como parte de convenios bilaterales entre los gobiernos de Estados Unidos y Bolivia. Existen programas y proyectos en toda Bolivia, con énfasis en las áreas rurales y población de bajos ingresos. Aproximadamente 100 millones de dólares en donaciones por año. USAID en Bolivia tiene cinco programas sectoriales (salud, democracia, medio ambiente, oportunidades económicas y desarrollo integral). Agencia de los Estados Unidos para el Desarrollo Internacional (2015): «*Programa de Cooperación USAID en Bolivia*» [en línea]: http://spanish.bolivia.usembassy.gov/usaid.html [Consulta: 07/05/2015]

El programa tiene como objetivos:

— Mejorar la atención de infecciones de transmisión sexual (ITS);

— Mejorar la capacidad de diagnóstico para ITS y,

— Promover el uso de condón.

Estos centros de especialidad de La Paz y Santa Cruz fueron dotados de laboratorios especializados para el diagnóstico de ITS, de reactivos para realizar múltiples estudios de seroprevalencia y dotar de reactivos a los centros de transfusión sanguínea. En 1992 se firma un convenio con el Ministerio de Salud y Previsión Social para el desarrollo del Proyecto Contra el SIDA (PCS) con los siguientes componentes:

— Fortalecimiento de los Servicios de control de ITS

— Servicio de Consejería

— Equipamiento de los servicios

— Capacitación de personal

— Información, Educación y Comunicación (IEC)

— Dotación de medicamentos y reactivos

— Vigilancia Epidemiológica

— Control sistematizado de las ITS en grupos vulnerables

— Promoción del uso de condón

El año 1994 se implementan estos centros en las ciudades de Oruro, Sucre, Potosí, Beni y finalmente Cobija (Pando). Se conforman equipos multidisciplinarios en cada centro, constituidos por médicos, bioquímicos, y psicólogos, para desarrollar un enfoque integral en la atención. Estos Centros de especialidad tuvieron el apoyo desde 1994 por el CCH (1994-1999), y se dio continuidad y fortalecimiento de estos centros a través del Proyecto de Salud Integral (PROSIN).

El Proyecto de Salud Integral, PROSIN, tuvo un rol muy importante en el desarrollo del Programa Nacional de ITS-VIH y SIDA del Ministerio de Salud y Deportes tanto en Programa Nacional como en la implementación en los nueve (9) departamentos de los Centros Departamentales de Vigilancia de ITS-VIH y SIDA dependientes de los SEDES.

La primera etapa de apoyo transcurre desde 1999 a 2001 en el contexto de las políticas nacionales contenidas en el Plan Estratégico

de Salud (PES) y en el marco de los resultados de USAID; se elabora el Plan Estratégico de la división del VIH/SIDA.

Los últimos diez (10) años, el Programa Nacional de ITS/VIH/SIDA recibió el apoyo técnico y financiero de las siguientes organizaciones:

— USAID/Bolivia-PROSIN-PROSIN II
— FONDO GLOBAL
— OPS/OMS
— UNICEF
— CDC de los Estados Unidos de Norteamérica
— DFID
— IMPACT
— MISIÓN ALIANZA NORUEGA

De acuerdo al comportamiento de esta pandemia, el Ministerio de Salud ha decidido llevar adelante una estrategia que permita:

— Estratificar las poblaciones de intervención de acuerdo a los comportamientos de riesgos y el acceso a estos grupos.
— Acceso y cobertura universal a los antiretrovirales.
— Mejorar la calidad de la atención.
— Instrumentar proyectos de prevención en poblaciones prioritarias.
— Acciones oportunas para reducir el estigma y la discriminación.
— Sensibilización social.

El Programa Nacional de ITS/SIDA del Ministerio de Salud y Deportes, a través de los nueve (9) Programas Departamentales de ITS/SIDA, ha registrado, a partir del 1984 hasta el tercer trimestre de la gestión 2005, 1.720 personas que viven con el VIH/SIDA en el país (Rimassa, M., Pérez, G. y Trujillo, L., 2007).

Santa Cruz es el departamento que ha notificado la tasa más alta de personas que viven con el VIH o SIDA, seguido por La Paz y Oruro. Santa Cruz ha notificado más de la mitad de las personas que viven con el VIH/SIDA registradas en el Ministerio de Salud. Estas notificaciones muestran solamente una parte de la verdadera situación. El sistema de notificación conoce un subregistro substancial, solamente toma en cuenta los servicios de salud que pertenecen al Ministerio de Salud.

Además, una persona puede vivir muchos años con el virus sin darse cuenta, porque no presenta síntomas y signos de enfermedad, y muchos médicos no toman en cuenta el diagnóstico del VIH si una persona se presenta con los primeros signos y síntomas de enfermedad. Recientemente, la OPS/OMS ha caracterizado la epidemia del VIH/SIDA en Bolivia como concentrada, que significa que la prevalencia ha superado el 5% en algunos grupos de la población[8].

Los grupos de edad más afectados son los entre 15 y 34 años de edad, con más del 60% de las notificaciones en el país. La transmisión sexual es la vía de transmisión más encontrada en Bolivia: el 95% de las personas notificadas se han transmitido el virus a través de relaciones sexuales. Tres por ciento es por medio de transfusiones de sangre o accidentes con objetos cortopunzantes y 2% son niños que viven con el virus por la transmisión vertical, de madre que vive con el VIH a su hijo. Dentro de la vía sexual, el 64% se ha transmitido el virus por relaciones heterosexuales, el 24% por relaciones homosexuales y el 11% por medio de relaciones bisexuales.

Esto no quiere decir que las mujeres no están a riesgo de contraer el VIH. Al contrario, las mujeres son más vulnerables que los hombres para la transmisión del VIH y otras infecciones de transmisión sexual. La primera razón es biológica; el órgano reproductivo de la mujer es muy vulnerable y el semen de un hombre que vive con el VIH contiene una concentración alta de virus. Por eso, la transmisión del VIH de hombre a mujer es más fácil que al revés (Organización Panamericana de Salud, 2008).

Las historias clínicas a la fecha se manejan en soporte papel, el Programa ITS-VIH/SIDA de La Paz cuenta con 10.000 historias clíni-

---

8 El trabajo del equipo constó de análisis de estudios realizados en el país, análisis de las notificaciones del Programa Nacional de ITS/SIDA, entrevistas con agencias y organizaciones trabajando en la temática y una reunión de expertos a nivel nacional. Los resultados del trabajo de tipificación de la epidemia realizado indican que Bolivia se encuentra en una epidemia concentrada 1: la prevalencia en algunos grupos de población que tienen comportamientos sexuales que les ponen a más riesgo para la transmisión del VIH, es por encima de 5%. Protto, J.P. et al (2008): *«Entorno epidemiológico y respuesta a la epidemia del VIH en Bolivia»* [en línea]: http://www.scielosp.org/pdf/rpsp/v23n4/v23n4a12.pdf [Consulta: 06/10/2014].

cas que son resguardadas en gaveteros, a cargo de la Jefe de enfermeras, quien es responsable de la seguridad de las mismas.

Gracias al financiamiento del Fondo Mundial[9] y la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) entre 2005-2006, se informatizan las historias clínicas del Programa ITS-VIH/SIDA de La Paz desde el año 1984 (que se presenta el primer caso de VIH/SIDA) hasta fines de 2006.

Todos los consultorios del Programa ITS-VIH/SIDA cuentan con una computadora e impresora gracias al Fondo Mundial[10]. Por falta de algu-

---

9 En junio de 2001, se realizó en Nueva York la Asamblea General de las Naciones Unidas sobre el VIH/Sida, con presencia de diferentes gobiernos, de representantes de organizaciones de la sociedad civil y personas con VIH de todo el planeta, para establecer una estrategia mundial que pueda responder con efectividad a la pandemia del sida. Se creó en esa ocasión el Fondo Mundial con el propósito de recolectar de 7.000 a 10 mil millones de dólares y apoyar a los programas de sida, malaria y tuberculosis en países de escasos recursos. La creación del Fondo Mundial con dinero donado por varios países ricos constituyó un evento importante en la historia de la humanidad, porque se destinaron fondos para que la sociedad civil, las personas afectadas con VIH/Sida, malaria y tuberculosis junto al Estado, lograran estructurar en cada país un espacio de trabajo conjunto, llamado «Mecanismo de Coordinación del País» (MCP) que acompañara todo el proceso para prevenir y combatir las tres enfermedades con los recursos donados. Es importante aclarar que el MCP no maneja fondos, para ese fin son elegidas, mediante rigurosos procesos de selección, las organizaciones llamadas «Receptor Principal». En Bolivia se estructuró el MCP con representantes del Gobierno y de la sociedad civil: compuesta por representantes de organizaciones de personas con VIH, organizaciones sociales como la CSUTCB, CIDOB, ONG, Iglesia y organizaciones internacionales de cooperación. Luego de meses de trabajo conjunto, elaboraron una propuesta de país para obtener 31,8 millones de dólares para cinco años, de los cuales 30 por ciento se programaron para el Gobierno, es decir, para los tres programas a cargo del Ministerio de Salud y Deportes; 25 por ciento para la sociedad civil; 20 por ciento a personas afectadas con VIH-Sida y el resto para universidades, iglesias y otras instituciones que tengan experiencia y deseen ejecutar proyectos que deben ganar su financiamiento en licitación pública realizada por el receptor principal con control del MCP. Organización Panamericana de la Salud-Bolivia (2007): *«VIH/SIDA, Gobierno y Fondo Mundial: cuestión de vida»* [fuera de línea]: http://www.ops.org.bo/cgi/sys/s2axic?DB=B&S2=2&S11=12911&S22=b [Consulta: 07/10/2008].

10 El Fondo Mundial ha financiado programas de prevención del VIH que mejoran los servicios de salud en Bolivia, mediante la dotación de equipos e

nas instalaciones, el Sistema de Información desarrollado no está siendo utilizado en la actualidad, llevándose a cabo el llenado de las historias clínicas en forma manual en el servidor por un encargado de sistemas.

El Programa ITS-VIH/SIDA envía cada mes toda la información en un reporte en forma cuantitativa al Director del Servicio Departamental de Salud (SEDES) La Paz y al Ministerio de Salud y Deportes para su conocimiento.

2.5.1 SITUACIÓN EPIDEMIOLÓGICA DEL VIH

Según el Programa Nacional de ITS/VIH/SIDA, la epidemia del VIH a diciembre de 2012 tenía las siguientes características: «La distribución de casos por departamentos revela que el 89% de los casos se distribuye en los departamentos de Santa Cruz, Cochabamba y La Paz, correspondiendo el 52% al Departamento de Santa Cruz (…). La relación hombre/mujer es de 1,7 a 1; es decir, que por cada 10 mujeres VIH(+) existen 17 hombres en igual condición. Seis de cada diez personas con VIH/SIDA tiene entre 15 y 34 años». La distribución de casos según departamentos, señala que el 52% se encuentra en Santa Cruz, 20% en Cochabamba y 17% en La Paz.

Los datos de prevalencia del VIH reportados por esta oficina señalan que 0,15% corresponde a la población general, 0,20% a las mujeres embarazadas, 0,57% a las trabajadoras sexuales, 11,60% a los HSH y GLTB y 19% a las mujeres transgénero.

Para fines de 2012, la misma oficina estatal reportaba que desde 1984-2012 se registraron en Bolivia 8.815 casos de VIH, lo cual implicaba un crecimiento progresivo y constante de la epidemia. Tan solo con referencia a la gestión 2011, se registra un incremento del 25%. Los datos mostraron que el eje troncal acumulaba el 89% del total de los caso de VIH.

---

insumos, contribuyendo a la detección y tratamiento de ITS VIH/SIDA. El Fondo Mundial ha sido, y continúa siendo, una de las fuentes de apoyo más importantes de la estrategia de control de ITS VIH/SIDA del Ministerio de Salud y Deportes. Asociación Ibis–Hivos (2008): *«Trabajo con personas viviendo con VIH/SIDA»* [fuera de línea]: http://www.ibis-hivos.net/tsc1.asp?seccion=pvvs [Consulta: 07/10/2008].

Según el Programa Nacional de ITS/VIH/SIDA para junio de 2013, el número de casos de VIH registrados en Bolivia aumentó a 10.162 con una prevalencia de 97 por millón de habitantes. Para fines de 2014, en base a información de la misma oficina, la prensa boliviana reportaba que el número de casos alcanzaba a 12.480

Tabla 1. Resumen del número de VIH registrado 2012-2014

Gestión	Casos de VIH registrados
1984-2012	8.818
1984-2013	10.162
1984-2014	12.400

Fuente de elaboración: REDBOL en base a informaciones del Programa Nacional de ITS/VIH/SIDA

De acuerdo con el Programa Nacional de ITS/VIH/SIDA, a fines de 2014 «…en Bolivia 4.104 personas que viven con VIH reciben tratamiento antirretroviral. El Gobierno nacional destinó el 80% del total del presupuesto asignado para esta causa en la compra de medicamentos durante el 2014, proyectando el 100%».

A pesar del aumento del número de personas viviendo con el VIH y que reciben TARV, los líderes de REDBOL continúan reportando serias vulneraciones a los derechos humanos[11]. Estas representan brechas económicas, programáticas e informativas que tienen relación con la falta de recursos, la desinformación, la falta de sensibilización, ausencia de políticas públicas con recursos económicos, falta de insumos inexistencia de capacitación y actualización del personal de salud y falta general de programas de educación para la población general (REDBOL, 2015).

---

[11] «Se proporciona el ejemplo de Nadia (nombre ficticio), una mujer de 24 años que fue detectada positiva al VIH en el momento del parto. Su experiencia hace referencia a las muchas violaciones y maltratos que muchas mujeres embarazadas con el VIH sufren hoy en día en los servicios materno-infantiles. Nadia aún no toma medicamentos ARV, está esperando los resultados de sus exámenes de Carga Viral y CD$. Su bebé recibe profilaxis, aún no se sabe si adquirió el VIH. La negación de atención del personal de salud, implicó que ella tuvo que nacer con un parto vaginal sin que Nadia se encuentre en TARV, lo cual le causa angustia, porque se encuentra segura que su hija nació con el VIH por su culpa» (REDBOL, 2015).

2.5.2 CENTROS DE VIGILANCIA, INFORMACIÓN Y REFERENCIA (CVIR)

El Programa Departamental ITS/VIH/SIDA, dependiente de la Unidad de Epidemiología del Servicio Departamental de Salud (SEDES) La Paz, desarrolla un conjunto de actividades orientadas a la promoción, prevención, control y vigilancia epidemiológica de las infecciones de Transmisión Sexual (ITS), VIH y SIDA.

Es responsable de la planificación, programación, evaluación y supervisión de las actividades, realiza una coordinación interinstitucional y multisectorial.

En el Nivel Departamental existen los Centros de vigilancia, información y referencia (CVIR), a nivel Departamental se denomina: CDVIR La Paz, y a nivel Regional: CRVIR El Alto, con personal técnico profesional capacitado y sensibilizado, donde se prestan servicios de atención a las personas afectadas por las ITS y el VIH/SIDA.

Se cuenta, para el funcionamiento de estos Centros, con el respaldo legal basado en la Ley 3729 de Prevención del VIH y SIDA y Protección a las Personas que viven con el virus del Sida (PVVS).

En 1992 el Ministerio de Salud y Deportes con el apoyo de USAID/BOLIVIA y los CDC de los Estados Unidos implemento una estrategia de prevención dirigida a poblaciones vulnerables, con la apertura de los Centros Departamentales de Vigilancia, Información y Referencia (CDVIR), iniciando este proyecto en una primera etapa en la ciudad de La Paz; posteriormente, este programa se extendió a las nueve (9) capitales y la ciudad de El Alto (1994) con el apoyo muy importante de PROSIN.

Se conforman equipos multidisciplinarios en cada CDVIR constituidos por médicos, bioquímicos y psicólogos para desarrollar un enfoque integral en la atención.

En el año 2003, entran en funcionamiento los CRVIR en ciudades fronterizas como Yacuiba (Tarija), Puerto Quijarro (Santa Cruz) y Guayaramerín (Beni).

El CDVIR tiene como misión: «Un programa departamental fortalecido, con incidencia y prevalencia disminuida de ITS/VIH/SIDA, con un recurso humano capacitador (educador) y sensibilizado, que ofrece una atención integral, universal, e interdisciplinaria, con un sistema de vigilancia y control eficaz, eficiente y de calidad para

las ITS/VIH/SIDA. Contribuyendo a mejorar la calidad de vida, a través de la promoción de la salud y prevención de la enfermedad, respetando la diversidad sexual, cultural y los derechos humanos, en el marco de la salud familiar comunitaria e intercultural».

El CDVIR tiene como objetivos:

— Mejorar la atención de ITS/VIH/Sida

— Mejorar la capacidad de diagnóstico de ITS/VIH/SIDA para el personal de los CDVIR con proyección a las Redes de Salud y Hospitales del área urbana y rural.

— Promover las Actividades de Prevención (uso del condón, discriminación, aspectos legales).

— Actividades de IEC.

El CDVIR presta los siguientes servicios:

— Servicio de atención médica a usuarios de la población general con ITS.

— Capacitación al personal de salud.

— Actividades educativas a la comunidad.

— Vigilancia epidemiológica.

— Atención a Trabajadoras Sexuales (TSA):

  • Control médico cada 15 días.
  • Laboratorio STAT cada 3 meses.
  • Prueba para VIH cada 6 meses.
  • Supervisiones a locales nocturnos.
  • Atención en enfermería: tratamiento supervisado.

El CDVIR lleva a cabo un manejo integral con Personas Viviendo con VIH (PVVS):

— Control médico a demanda

— Triaje en enfermería

— Entrega de ARV

— Exámenes de Laboratorio

— Apoyo nutricional

— Apoyo psicológico

— Consejería

— Trabajo Social
— Información sobre ITS/VIH/SIDA
— Adherencia a la terapia antirretroviral
— Referencia a Hospitales de segundo o tercer nivel.

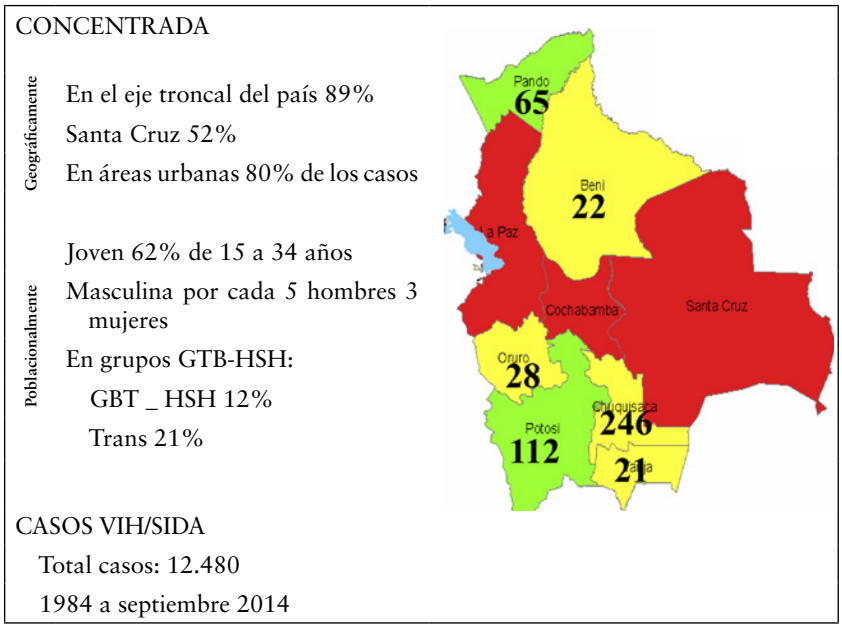

Figura 4. Casos de VIH-SIDA en Bolivia

Fuente de elaboración: CDEVIR (2015).

En Bolivia, el tratamiento de personas que viven con VIH no es el adecuado, existen pacientes que pasan de centro de salud a otro, las instancias del CDVIR, al ser de manejo ambulatorio, coordina la atención de los pacientes mediante órdenes de referencia para su atención en la especialidad requerida, en los diferentes establecimientos; sin embargo, dicha atención no es brindada; en varias ocasiones los pacientes regresan a instancias de CDVIR sin haber recibido la atención requerida.

Por otro lado, existe actualmente un porcentaje elevado de desconocimiento sobre las medidas de seguridad que se deben tener para tratar a personas que viven con VIH, tanto por el personal médico, como por otras personas que llegan hasta estigmatizar la enfermedad,

por lo que se da un alto índice de vulneración de derechos de estas personas; el CDVIR trabaja la parte preventiva, precisamente mediante las ferias y campañas que se realizan en diferentes espacios de concentración masiva, dando orientación pertinente además de la realización de pruebas rápidas (CDVIR, 2015).

2.5.3 RED DE PERSONAS QUE VIVEN CON EL VIH EN BOLIVIA-REDBOL

La caída del financiamiento para VIH a nivel internacional fue sentido por los países que aún registran entre un 75%-100% de dependencias de la cooperación internacional en VIH, como es el caso de Bolivia. Esta realidad sucedió en aquellos países que inmediatamente después de haber superado la categoría de «pobreza extrema», tuvieron que asumir responsabilidades que corresponden a países con economías más estables, es una problemática actual, no solamente para el financiamiento disponible para el VIH, sino para la salud en general.

Según el Ministerio de Economía y Finanzas, el crecimiento de los indicadores macroeconómicos de Bolivia posicionó a Bolivia dentro de la categoría de Países de Ingresos Medios, dejando de ser un país de «pobreza extrema». Esta categorización macroeconómica, tuvo implicancias directas en la capacidad de recibir recursos de la cooperación internacional para el VIH. En otras palabras, en la medida que en Bolivia crece la macroeconomía, se tiene menos posibilidades de acceder a recursos de la cooperación internacional.

A pesar que se cuenta con un marco legal sólido, una Ley específica para el VIH (Ley 3729) y un Reglamento, en la práctica no se implementan adecuada y oportunamente, no se ha logrado la exigibilidad de los derechos humanos protegidos en la Ley ni en la Constitución Política del Estado (REDBOL, 2015).

En el año 2000 se funda la Red Nacional de Personas Viviendo con el VIH-SIDA en Bolivia-REDBOL, pero se organiza e implementa sistemáticamente desde fines de 2012, consciente de la progresiva retirada de la cooperación internacional de Bolivia, este proyecto tuvo el objetivo de buscar la sostenibilidad de los servicios fundamentales para la prevención del VIH y para la sobrevivencia de las personas viviendo con el VIH.

A fines de 2012, REDBOL presentó una solicitud de financiamiento a HIVOS Holanda- Oficina Regional Sud América, la misma que estaba orientada a lograr la asignación de recursos para los programas de prevención y atención del VIH, independiente de la cooperación internacional. La demanda se basó en la exigencia del cumplimiento de las responsabilidades del Estado para la protección del derecho humano a la vida, la salud y a la dignidad. Durante los dos (2) primero años de implementación del proyecto (2012- 2013) se trabajó sensibilizando a las esferas estatales, facilitando la producción de estudios de base que sirvieron para el diseño del Plan de Incidencia Política de REDBOL para la asignación de recursos en VIH 2012-2014 (PIP) y capacitando a las y los líderes en incidencia política (IP).

2.5.4 FACTORES SOCIO-POLÍTICOS

A pesar de los anuncios optimistas del Gobierno sobre el gran crecimiento económico sirvió para ahuyentar a la cooperación internacional; los líderes en Bolivia siguen reportando gravísimas fallas en la protección de los derechos humanos, particularmente el derecho a la salud y a la vida, en contra de las personas que se encuentran viviendo con el VIH, hecho que se evidencia en particular en los lugares de atención como ser hospitales públicos, situación que no ha disminuido con el crecimiento macroeconómico.

Al mismo tiempo, existe una política de gobierno con la cooperación internacional cada vez más intransigente, la cual tiene el efecto de eliminar las pocas agencias que apoyan a las organizaciones de base comunitaria.

Por otra parte, las nuevas regulaciones para las ONG están generando muchos obstáculos para la existencia de las organizaciones de base comunitarias.

Por último, 2015 marca el año de conclusión de la Ronda 9 de financiamiento del Fondo Mundial para Bolivia. Bolivia puede volver a postular, pero primero debe recuperar la elegibilidad del MPC. La reconstitución del Mecanismo Coordinación País Bolivia MPC-Bolivia ha demostrado ser un desafío grande ya que requiere la participa-

ción y consenso de varios actores[12]. Además, el Fondo Mundial ha dispuesto la cifra tope de 41 millones de dólares para Bolivia, monto que se debe distribuir entre las tres (3) enfermedades VIH, Tuberculosis y Malaria (REDBOL, 2015).

2.6 SISTEMA NACIONAL DE INFORMACIÓN EN SALUD (SNIS)

2.6.1 ANTECEDENTES

El Sistema Nacional de Información en Salud y Vigilancia Epidemiológica (SNIS-VE) es un conjunto de instrumentos, procedimientos y herramientas destinados a la captación, sistematización, consolidación, procesamiento, retroalimentación, análisis y difusión de datos e información para la gerencia y la vigilancia epidemiológica que permitan tomar decisiones adecuadas y oportunas en la planificación, ejecución y evaluación, de políticas públicas en el ámbito de la salud.

Fue creado en 1990 a partir de la Dirección Nacional de Planificación y Proyectos del MPSS, en principio en forma muy rudimentaria en base a variables básicas que en aquel momento se constituían las necesarias para el seguimiento de las acciones prioritarias de salud, su procesamiento bajo un sistema manual con la utilización del paloteo para la sistematización y consolidación de los datos y su transformación en información.

---

12 «Bolivia es uno de los países de América Latina que menos invierte en la respuesta al VIH y el SIDA con sus recursos domésticos y tiene la mayor dependencia de la solidaridad internacional por medio de donaciones de medicamentos e insumos de países hermanos, subvenciones de la cooperación internacional, incluyendo el financiamiento del Fondo Mundial. Sin el apoyo internacional, miles de personas viviendo con VIH/Sida en Bolivia estarían condenadas a morir de complicaciones relacionadas con el SIDA como resultado de un Estado ausente». Los Tiempos (2014). «VIH, Tuberculosis y Malaria: Bolivia en riesgo de perder 41 millones de dólares» [En línea]:

http://www.lostiempos.com/oh/actualidad/actualidad/20140712/vih-tuberculosis-y-malaria-bolivia-en-riesgo-de-perder-41-millones-de_266376_583958.html [Consulta: 23/09/2014]

A partir del año 1985, se comienzan a utilizar algunas herramientas como el Diagnóstico Comunitario en los puestos de salud, efectuado por auxiliares de enfermería y médicos de provincia del Plan Integrado de Actividades de Áreas de Salud (PIAAS) de aquel entonces, que posteriormente se denominó Módulo de Información Básica, instrumento hasta la actualidad vigente y de gran valía para el Sistema Nacional de Salud.

El proceso del diseño del SNIS tiene su inicio en la Primera Reunión Nacional de Planificadores, realizada en la ciudad de Santa Cruz de la Sierra, del 19 al 21 de Julio de 1990, donde se conformó una «Comisión Nacional» encargada de sistematizar las experiencias regionales en el manejo de la información y el diseño de una propuesta.

Finalmente, el 29 de Octubre de 1990, en la misma ciudad, se aprobó la propuesta final y es en este histórico evento que se adoptó el nombre oficial de «Subsistema Nacional de Información en Salud, SNIS» y se aprobó el funcionamiento de los «Comités de Análisis de la información (CAI)» en cada nivel Gerencial del Sistema (en ese entonces, Área de Salud, Distrito, Región y Nivel Central) (Armijo *et al.,* 1993).

A partir del año 2000, se introduce el SNIS de II generación y la introducción de la normativa funcional del ciclo de la información hasta ahora vigentes, los instrumentos de sistematización y los de consolidación con una mayor cantidad de variables, así como la consolidación del manejo de la vigilancia epidemiológica. En los últimos años a partir del año 2006, este avance es más notorio con la implementación de la tecnología a través de la plataforma de comunicaciones e introducción de las herramientas informáticas que coadyuvan a la sistematización de los datos.

Durante la gestión 2010, es efectuado el último proceso de evaluación al SNIS-VE planteándose su reestructuración en la perspectiva de la construcción del Sistema Único de Información en Salud y reflexión profunda de los procesos, procedimientos, instrumentos y flujos con los cuales se desenvolvía la información, de esta manera son introducidas herramientas tecnológicas de procesamiento automático como punto de unificación de la información de las principales líneas fuerza de la política nacional (seguros públicos de salud, programa desnutrición cero y bono Juana Azurduy) enfocados en los procesos de captación y sistematización de la información coadyuvando a la

obtención de información agregada y desagregada desde el establecimiento de salud, propiciando la evitación de duplicación del dato, mejoramiento de la calidad de la información y la agilización de la gestión de la información; proceso traducido en el procesamiento manual de la información con la reducción, integralidad y compatibilidad de los diversos instrumentos ya existentes en el sistema de información. Es incorporada la carpeta familiar como instrumento básico de la política nacional a la gestión de la información, es implementado el certificado único del recién nacido y mejorado los registros para la mortalidad general y perinatal.

El SNIS es la unidad responsable de proveer al país y al sector salud de datos e información para la gerencia y la vigilancia epidemiológica que permitan tomar decisiones adecuadas y oportunas en la planificación, ejecución y evaluación, de políticas públicas en el ámbito de la salud.

2.6.2 MARCO LEGAL

El Sistema nacional de información en Salud está bajo el siguiente respaldo legal:

Ley del Sistema Nacional de Información Estadística (SNIE) –DL 14100 de fecha 5 noviembre de 1976– la misma confiere al Instituto Nacional de Estadística (INE) la responsabilidad de dirigir, planificar, ejecutar, controlar y coordinar las actividades estadísticas del sistema; promover el uso de registros administrativos, tanto en oficinas públicas como privadas, para obtener datos estadísticos; además de capacitar recursos humanos y crear la conciencia estadística nacional. En este contexto, el INE se ha estructurado orgánicamente para realizar su trabajo y cumplir con sus objetivos institucionales.

Es así que el Sistema Nacional de Información en Salud (SNIS) forma parte del SNIE, siendo catalogado por el INE en la actualidad como modelo demostrativo de un sistema de información basado en registros administrativos.

La Ley 031 Marco de Autonomías y Descentralización «Andrés Ibáñez» de fecha 19 de julio de 2010 establece como régimen competencial el artículo 81 (Salud), en función a los artículos 304 y 299 de la CPE:

— Los Gobiernos indígena originario campesinos deben proporcionar información sobre la medicina tradicional desarrollada en su jurisdicción al «Sistema Único de Información en Salud» y recibir la información que requieran en aplicación del principio de lealtad institucional.
— Los Gobiernos departamentales autónomos deben informar al ente rector nacional del sector salud y las otras entidades territoriales autónomas sobre todo lo que requiera el «Sistema Único de Información en Salud» y recibir la información que requieran.
— Los Gobiernos municipales autónomos deben proporcionar información al «Sistema Único de Información en Salud» y recibir la información que requieran, a través de la instancia departamental en salud.

2.6.3 MARCO INSTITUCIONAL

El Sistema nacional de Información en Salud (SNIS) tiene como misión: «*Somos un área técnica del Ministerio de Salud y Deportes que regula, norma y administra la gestión de la información en salud destinada a la gerencia, la vigilancia de la salud pública y el análisis de la situación de salud para la toma de decisiones en los diferentes niveles del sistema de salud*».

Las competencias asignadas al SNIS son:

— Realizar tareas de planificación
— Articular acciones con organismos externos
— Realizar administración de recursos
— Elaborar estudios de investigación
— Control en temas epidemiológicos
— Deberá realizar tareas de legista y suministros de insumos
— Garantizar el buen desenvolvimiento de sus recursos humanos

2.6.4 ESTRUCTURA ORGANIZACIONAL

El Sistema Nacional de Información en Salud (SNIS) cuenta con un Manual de Organización y Funciones que describe las tareas específicas que se deben cumplir en cada uno de los niveles y jerarquías de

su estructura organizacional. Esta estructura está reflejada en el siguiente organigrama:

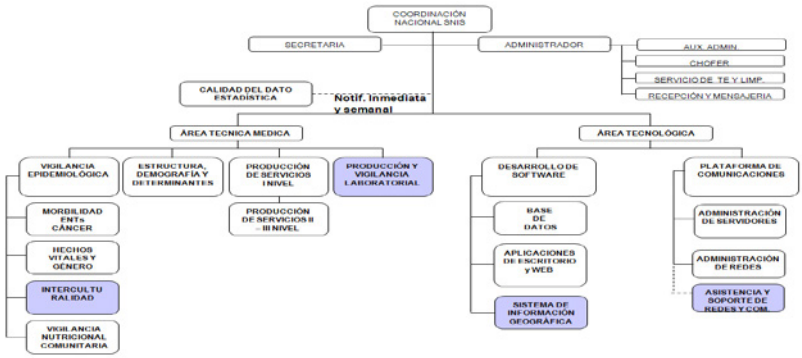

Figura 5. Organigrama Sistema Nacional de Información en Salud-Vigilancia Epidemiológica

Fuente de elaboración: Sistema Nacional de Información en Salud.

2.6.5 ÁREAS DEL SNIS-VE

Tabla 2. Áreas del SNIS-VE

Área	Objetivo
Estructura	Dotar al SNIS y al sistema de salud de información actualizada sobre factores condicionantes y determinantes que pueda ser utilizada para la Vigilancia Epidemiológica y la comunitaria así como para el Análisis de Situación de Salud.
Producción y Servicios	Normar y controlar la captación, sistematización, consolidación y difusión de los datos y la información relacionados con la producción de servicios para facilitar la toma de decisiones gerenciales y de vigilancia epidemiológica, en todos los niveles de atención y administrativos del Sistema Nacional de Salud. Esta información permite a los establecimientos de salud realizar la planificación, ejecución y control de sus actividades.

Área	Objetivo
Vigilancia Epidemiológica	Mejorar los procedimientos de la vigilancia epidemiológica (notificación, procesamiento, análisis y comunicación de la información), así como los procedimientos para el Análisis de la Situación de Salud (ASIS), en todos los ámbitos del Sistema Nacional de Salud.
Control de Calidad	Garantizar información estadística en salud confiable y de calidad, además de proporcionar instrumentos técnicos para el control de todos los procesos de organización y funcionamiento, en todos los niveles y subsectores de salud.

Fuente de elaboración: Sistema Nacional de Información en Salud

2.6.6 ORGANIZACIÓN DE LA RED DE INFORMACIÓN DEL SISTEMA

Todos los Establecimientos de Salud son considerados como unidades básicas de información estadística del sistema; es decir, los Puestos de Salud, Centros de Salud, Hospitales Básicos, Hospitales Generales, Hospitales de Especialidad e Institutos Nacionales, Públicos y Privados. En cada uno de los establecimientos de salud, los datos son recolectados, sistematizados, consolidados, analizados y difundidos mediante el sitio Web del SNIS y los anuarios de divulgación, para su uso por el Ministerio del sector, usuarios externos e internos del propio sistema de información.

2.6.7 FLUJO DE LA INFORMACIÓN

Los datos generados por el sistema nacional de información en salud siguen una ruta que pasan por diferentes etapas y niveles. En base a la norma vigente del SNIS-VE, el flujo traduce el proceso de transformación de datos a información en un lapso determinado, tomando en cuenta los niveles de atención y gestión del sistema de salud.

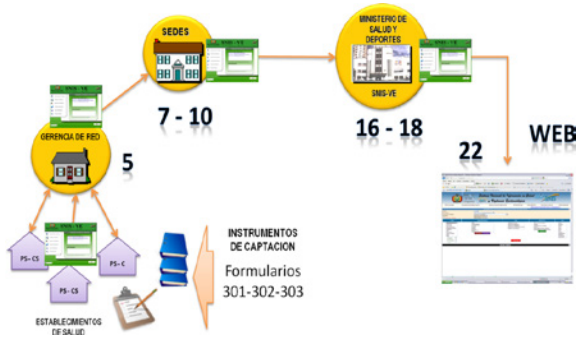

Figura 6. Flujo de información

Fuente de elaboración: Sistema Nacional de Información en Salud.

2.6.8 INSTRUMENTOS DEL SNIS

El Sistema Nacional de Información en Salud (SNIS) utiliza cuatro tipos de instrumentos o formularios de captura para registrar los eventos del sector que son:

— *Instrumentos de Captación:* Son los que están diseñados para el registro de datos de tipo clínico y están relacionados con la atención a usuarios o clientes de un servicio, denominado consumo del Servicio o Bien Físico. En este tipo de instrumentos se captan los datos socio-demográficos, Carnet de Vacunación, Carnet de Salud e Historia Clínica de cada paciente (datos no estadísticos, porque no están agregados).

— *Instrumentos de Sistematización:* Son instrumentos destinados al acopio continuo de datos estadísticos durante un periodo de tiempo definido, que permiten obtener al final de cada periodo información estadística organizada.

Tabla 3. Instrumentos del SNIS-VE, según el ciclo de información

Captación	Sistematización	Consolidación
Historia Clínica Básica	Cuadernos del SNIS-VE:	Formulario 301 Informe mensual de producción de servicios.

Captación	Sistematización	Consolidación
Historia clínica Perinatal	Cuaderno n.º 1 de registro de la consulta externa para centros de salud.	Formulario 303 informe mensual de producción de servicios laborales.
Recibo-recetario	Cuaderno n.º 2 de registro de la consulta prenatal, parto y puerperio.	
Carnet de salud infantil	Cuaderno n.º 3 del registro de las acciones de anticoncepción, prevención de ITS y del Cáncer de Cuello Uterino.	
Registros de vacunas	Cuaderno n.º 4 del registro de la atención integral de atención al menor de 5 años.	
Epicrisis y otros	Cuaderno n.º 5 del registro de las internaciones. Cuaderno n.º 6 del registro de las acciones de emergencias y enfermería. Cuaderno n.º 7 del registro de las atenciones odontológicas. Cuaderno n.º 8 del registro de la consulta externa y enfermería para puestos de salud.	

Fuente de elaboración: Sistema Nacional de Información en Salud.

Entre estos instrumentos se tienen los siguientes:

— CUADERNO n.º 1. CÓDIGO R.A. SALUD-INE 201: Registro de Consulta Externa, para Centros de Salud y Hospitales Básicos.

— CUADERNO n.º 2. CÓDIGO R.A. SALUD-INE 202: Control Prenatal y puerperio, para Centros de Salud y Hospitales Básicos.

— CUADERNO n.º 3. CÓDIGO R.A. SALUD-INE 203: Planificación Familiar y Atención de la Mujer No Gestante.

— CUADERNO n.º 4. CÓDIGO R.A. SALUD-INE 204: Registro de Parto y Recién Nacido.

— CUADERNO n.º 5. CÓDIGO R.A. SALUD-INE 205: Registro de Hospitalizaciones en Centros de Salud y Hospitales Básicos.

— CUADERNO n.º 6. CÓDIGO R.A. SALUD-INE 206: Registro de Consultas Odontológicas.

— CUADERNO n.º 7. CÓDIGO R.A. SALUD-INE 207: Registro sobre Nutrición y Desarrollo Infantil.

— CUADERNO n.º 8. CÓDIGO R.A. SALUD-INE 208: Registro sobre Enfermería, para Centros de Salud y Hospitales Básicos.

— CUADERNO n.º 9. CÓDIGO R.A. SALUD-INE 209: Registro sobre Emergencias atendidas.

— CUADERNO n.º 10. CÓDIGO R.A. SALUD-INE 210: Registro de Actividades con el Personal de Salud y la Comunidad.

— CUADERNO n.º 11. CÓDIGO R.A. SALUD-INE 211: Registro de Consulta Externa y Enfermería.

Instrumentos de Consolidación: Son formularios que centralizan datos estadísticos de cada establecimiento de salud al final de cada periodo (mensual), para su envío al siguiente centro de acopio que es la Gerencia de Red y finalmente al Servicio Departamental de Salud (SEDES), Departamento de Estadística. Estos formularios tienen la finalidad de depurar los datos, consolidar la información de un periodo de trabajo y facilitar la informatización de datos.

— Entre los instrumentos principales se tiene:

— FORMULARIO, CÓDIGO R.A. SALUD-INE 301, Informe Mensual de Producción de Servicios.

— FORMULARIO, CÓDIGO R.A. SALUD-INE 302, Informe Semanal de Notificación para la Vigilancia Epidemiológica.

— FORMULARIO, CÓDIGO R.A. SALUD- INE 303, Informe mensual de Laboratorio. Datos de Producción y Vigilancia Epidemiológica.

Instrumentos de Retroalimentación: Estos instrumentos tienen la finalidad de controlar la administración de un nivel gerencial determinado. Están diseñados para facilitar la lectura de la información procesada. Estos instrumentos son medios para informar los resultados del proceso productivo y establecer mecanismos de control, como el monitoreo y evaluación de resultados (Ministerio de Salud y Deportes, 2010).

2.6.9 EL CICLO DE LA INFORMACIÓN EN EL SNIS

El SNIS considera el ciclo de la información en una serie de momentos dispuestos en forma secuencial y articulados entre sí, que van desde el momento del registro o captura de los eventos y actividades que cumplen los servicios de salud, hasta el uso final de la información por parte del sistema y el sector, cuyo esquema es el siguiente: a) La captación de los datos, b) La sistematización, c) La consolidación, d) El procesamiento estadístico, e) el análisis de resultados, y f) La difusión para su uso en la planificación. Este proceso de momentos se ha adoptado debido a su flexibilidad y porque permite hacer ajustes periódicos, con el fin de asegurar la calidad de la información. A continuación se grafica el ciclo de la información (Ministerio de Salud y Deportes, 2010).

Figura 7. Ciclo de la información en el SNIS

Fuente de elaboración: Sistema Nacional de Información en Salud.

El manejo de los datos se organiza en el llamado «Ciclo de la información». Es importante destacar la dinámica circular del ciclo, ya que traduce la secuencia de procesos que permanentemente van alimentando al subsiguiente.

2.6.10 SISTEMAS DEL SNIS-VE

Los sistemas con que cuenta el SNIS-VE son los siguientes:

— *Sistema de Atención Primaria en Salud (SOAPS):* Registra los antecedentes básicos de filiación de las personas que son atendidas en el servicio (datos socio-demográficos, Carnet de Vacunación, Carnet de Salud e Historia Clínica de cada paciente); asimismo, están relacionados con la atención a usuarios o clientes de un servicio, denominado consumo del Servicio o Bien Físico.

— *Sistema de Información de Clínico Estadístico (SICE):* Automatiza el proceso de admisión de pacientes, registro de datos de consulta externa, internación y servicios complementarios de hospitales de segundo y tercer nivel.

— *Sistema Recursos Humanos (SOREHH):* Registra el personal que trabaja en los Establecimientos de Primer, Segundo y Tercer nivel del Sistema de Salud.

— *Hechos Vitales:* Establecimiento del área de Hechos Vitales dentro el SNIS-VE y en los diferentes departamentos con la finalidad de fortalecer las estadísticas vitales a través de la implementación de instrumentos estandarizados en coordinación con el registro civil y otras instituciones relacionadas con la Salud.

2.6.11 LA INFORMACIÓN ESTADÍSTICA QUE GENERA EL (SNIS)

La información que se genera en el sistema sobre los eventos y casos atendidos y practicados en el sector están expresados en forma de números absolutos, indicadores (proporciones, porcentajes y tasas), cuadros y gráficos.

Los principales resultados y productos publicados en el sitio Web del SNIS y en los anuarios son los referidos a los siguientes temas:

2.6.11.1 **Casos Atendidos**

— *Atención Integral al menor de 5 años:*

- Control de Crecimiento y Desarrollo a Niños menores de 5 Años.
- Coberturas de Control de Crecimiento y Desarrollo en menores de 5 años, por Áreas de Salud.
- Estado Nutricional en Niños Menores de 5 años.
- Desnutrición General y Moderada-Severa en Menores de 5 años.
- Vacunación y Coberturas Pentavalente, Antipolio, BCG a Niños Menores de 1 año.
- Coberturas de Vacunación Pentavalente 3ra. Dosis en Niños Menores de 1 año.
- Municipios en Riesgo de Vacunación 3ra. Dosis Pentavalente a Niños Menores de 1 año.
- Vacunación y Coberturas SRP a Niños de 12 a 23 Meses.
- Coberturas de Vacunación SRP a Niños de 12 a 23 Meses.
- Municipios en Riesgo de Vacunación Dosis de SRP a niños de 12 a 23 meses.
- Distribución y Coberturas de Micronutrientes.
- Episodios de Diarrea y Tasa por Mil en niños Menores de 5 años.
- Episodios Diarreicos Atendidos por 1.000 en Menores de 5 años.
- Casos de Neumonía y Tasa por Mil en niños Menores de 5 años.

— *Atención Integral a la Mujer:*

- Consultas Prenatales e Indicadores en Mujeres Embarazadas.
- Relación de Coberturas de Control Prenatal Nuevos.

- Atención de Partos en Servicios e Indicadores.
- Relación de Partos Atendidos en Servicio, por Personal de Salud y Partera Capacitada en Domicilio.
- Relación de Partos Institucionales e Índice de Cesáreas.
- Relación de Embarazos Esperados, Control Prenatal de Nuevos, Embarazadas c/4 Controles y Atención de Partos.
- Indicadores de Salud Sexual y Reproductiva.
- Toma de Muestra para Estudio Citológico (PAP).
- Vacunación y Coberturas de Toxoide Tetánico a Mujeres en Edad Fértil.

— *Producción de Servicio:*

- Relación de Consulta Externa Nuevas y Repetidas e Indicador.
- Relación de Consulta Externa Nuevas y Repetidas e Indicador, según niveles de Atención en Salud.
- Relación de Consultas y Actividades Odontológicas.

— *Atención del Sistema Universal Materno Infantil –SUMI:*

- Porcentaje de Atenciones Prestadas SUMI.
- Prestaciones por Niveles de Atención SUMI.
- Porcentaje de Ejecución de FOPOS en relación al desembolso CMS según Municipio.
- Número de Municipios según rangos de % de Ejecución de FOPOS en relación al Desembolso a CMS.
- Porcentaje de Pago Municipal en relación a Copos Facturados según Municipios.

— *Epidemiologia:*

- Casos sospechosos de Sarampión según Municipios.
- Indicadores de Calidad de Vigilancia del Sarampión.
- Casos sospechosos de Parálisis Flácida según Municipios.
- Vigilancia Epidemiológica de la Rubeola según Municipios.
- Casos sospechosos de Difteria según Municipios.
- Casos sospechosos de Tos ferina según Municipios.

- Cobertura de Vacunación antirrábica según Municipios.
- Incidencia de Leishmaniosis en todas sus formas por Mil Habitantes según Municipios.
- Área Endémica de Chagas según Municipios.

— *Análisis de Situación en Salud:*

- Porcentaje de Partos Atendidos en Servicio según Municipios.
- Porcentaje de Partos Atendidos en Domicilio por personal de salud según Municipios.
- Cobertura de Parto Institucional según Municipios.
- Porcentaje de M.E.F. que reciben Orientación en Planificación Familiar según Municipios.
- Cobertura de Vacunación 2da. Dosis de Toxoide Tetánico a Mujeres en Edad Fértil según municipios.
- Incidencia de Abortos en relación a Población de Embarazos Esperados según Municipios.
- Tasa de Mortalidad Materna por 1.000 Nacidos Vivos (reportados) según Municipios.
- Violencia Intrafamiliar 10.000 en Niños menores a 5 años (reportados) según Municipios.
- Violencia Intrafamiliar 10.000 a Mujeres (reportados) según Municipios (Ministerio de Salud y Deportes, 2010).

2.6.11.2 **Recolección y sistematización de los datos en el SNIS**

Las fuentes de datos que alimentan al sistema son las provenientes del ámbito de la consulta médica en cada uno de los establecimientos de salud (unidad primaria) y las brigadas de salud fuera del servicio con proyección de sus actividades en la comunidad. Actualmente estas fuentes de datos constituyen los centros más importantes de información básica por su volumen, representatividad y continuidad en el sistema.

El primer momento del ciclo de información (captura) está dado por la recolección de datos básicos de las actividades cumplidas por el personal de salud y de la comunidad. Esta información es captada por una serie de formularios, cuadernos y registros de sistematización diseñados para este fin.

La sistematización de los resultados se realiza en los formularios durante un período de tiempo definido (un mes) en los Cuadernos de Control n.º 1 al n.º 11 según el tipo de consulta médica.

La consolidación de los datos se la realiza en el formulario 301, Informe Mensual de Producción de Servicios y en el formulario 302, Informe Semanal de Notificación para la Vigilancia Epidemiológica, para su reporte a las respectivas Redes de Salud (donde existe un técnico estadístico) y luego a los Servicios Departamentales de Salud (SEDES) correspondientes, para el procesamiento y análisis de los datos centralizados en la unidad de cómputo, para luego reportar al SNIS nacional para la globalización de los reportes departamentales.

Finalmente, para cerrar el ciclo de momentos, el Ministerio de Salud-Servicio Nacional de Información de Salud luego de efectuar los controles de calidad, procesar, tabular los cuadros estadísticos y analizar los resultados finales en la unidad de cómputo nacional, los difunde mediante el Sitio Web del SNIS y los Anuarios Estadísticos de Salud, para ser utilizados por usuarios internos y externos al sector.

Las acciones que cruzan transversalmente a los momentos descritos son:

— El archivo de la documentación;

— La trascripción y revisión de los datos;

— El control de calidad de la información y la

— Retroalimentación al sistema (Ayala, 2013).

2.6.12 PLATAFORMA DE COMUNICACIONES

— La Plataforma de Comunicaciones brinda información mediante los servicios de correo electrónico, telefonía IP, Internet, y otros servicios.

— La plataforma de comunicación conecta al Ministerio con los Servicios Departamentales de Salud (SEDES), instituciones de salud (Hospitales, programas de salud).

— La plataforma brinda el soporte tecnológico para los sistemas de salud, página web.

— Centraliza las Bases de Datos.

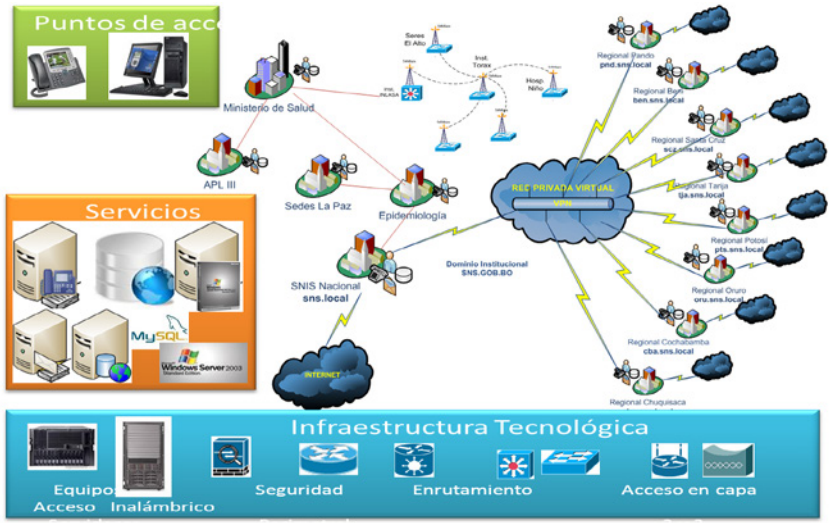

Figura 8. Estructura de la plataforma de comunicación

Fuente de elaboración: Sistema Nacional de Información en Salud.

2.6.12.1 Unidad de Cómputo

El sistema informático que se utiliza en el SNIS es obsoleto y retrasa el procesamiento de datos para su difusión según cronograma de entregas. Existe la urgente necesidad de sustituir los equipos con otros de mayor capacidad y velocidad (equipos de última generación), con el fin de cumplir oportunamente con su entrega y difusión a las autoridades del Ministerio de Salud y a los usuarios del entorno al sistema de información en salud.

En este mismo tema, se ha podido detectar la necesidad de dotar al sistema un tendido de red ágil, que articule a todas las unidades del SNIS desde los centros de salud (generadores primarios de información), gerencias de red y SEDES, a fin de maximizar los «tiempos y movimientos» en el procesamiento de los datos.

Se tienen planes para lograr, en el corto plazo, una tecnología de punta y moderna que permita encarar los trabajos de procesamiento con mayor oportunidad, precisión y confiabilidad.

Se espera que el requerimiento formulado se efectivice lo más pronto posible. El propósito es llegar con el flujo de información hasta los centros y establecimientos de salud del sistema.

En materia de recursos humanos, se ha podido observar que existe muy escasa motivación al personal técnico en cuanto a capacitación y actualización en los nuevos avances en informática (software). A nivel de las gerencias de red, los recursos no son los suficientes para cumplir con más oportunidad las actividades definidas en el manual de organización y funciones del SNIS. Se requiere renovar los equipos de trabajo del personal técnico en un número suficiente.

Si bien el personal de la unidad de cómputo tiene el perfil necesario, se requiere de una capacitación para reforzar la capacidad técnica sobre todo en la resolución de problemas que se presentan en el proceso. Este componente tan importante está ausente en el sistema.

Una manifiesta debilidad en el proceso es el hecho de que los centros y establecimientos de salud no cuentan con el personal adecuado para cumplir con las funciones de captura de los datos primarios, además del recargado trabajo que tiene el escaso personal en estas unidades de salud. Por esta razón, muchas veces los reportes llegan con retraso, lo que repercute en los desfases de cronograma en la centralización de los datos.

La unidad de cómputo no cuenta con el material suficiente para el desempeño de sus actividades. Se requiere dotar periódicamente los recursos materiales a fin de no interrumpir su labor.

Finalmente, un aspecto importante detectado es el hecho de los cambios permanentes de un año a otro, sobre las variables que se insertan en los cuestionarios, afectando el seguimiento de las series cronológicas de datos, además de la permanente revisión de los programas informáticos. Se revisan cada vez los programas informáticos en la mayor parte de los casos a principios de año (Ayala, 2013).

2.6.12.2 Software que se utiliza para el procesamiento en el sistema

El sistema informático (*software y hardware*) que se utiliza actualmente en el SNIS es obsoleto y retrasa el procesamiento de datos para su difusión oportuna de datos. Este hecho refleja la urgente necesidad de sustituir los equipos de última generación.

El software que se utiliza, que es un software propio del sistema, instalable en cualquiera de los niveles del sistema, tiene dos vías de acceso:

a) Solo para el ingreso de datos básicos

b) Solo para consulta de información de usuarios.

También dispone de un módulo de «generación de indicadores» de los diferentes eventos de salud atendidos por el sector (proporciones, razones, tasas para coberturas). Por otra parte, el módulo de «reportes» trabaja bajo el sistema de «cubo de datos» (*DB Cube*) que es una aplicación multidimensional, donde el usuario puede elegir los cuadros estadísticos y variables que requiera para su investigación.

Los hospitales del sistema procesan sus datos aplicando los *softwares* SIAP y SICE, que son paquetes especializados para la administración hospitalaria y para elaborar los reportes de sus actividades.

En este componente, se ha visto la necesidad de dotar al sistema un tendido de red ágil a nivel nacional, que articule a todas las unidades del SNIS, desde los centros de salud hasta los SEDES departamentales, con el fin de maximizar los procesos. Toda esta innovación tendría que estar acompañada de una capacitación permanente al personal encargado de estas unidades (Ministerio de Salud y Deportes, 2010).

2.6.12.3 Llenado de Formularios

El llenado de los formularios del SNIS, por parte del personal encargado, se puede resumir en los siguientes aspectos:

— Con relación a los formularios de recolección de datos que utiliza el SNIS, se pudo advertir que en muchos casos se presentan dificultades en su manejo y llenado, pese a tener los instructivos en el reverso de cada uno de ellos. Esta dificultad es el re-

sultado de la «falta de capacitación» teórica y práctica al personal encargado de las tareas de captura de la información primaria en los formularios descritos anteriormente.

— Casi la totalidad de los funcionarios encargados de realizar estos registros, manifestaron la necesidad de recibir una capacitación continua en el llenado de los formularios de captura, puesto que éstos también sufren modificaciones permanentes en su contenido (cambios o incrementos de variables).

— Una parte importante de los funcionarios manifestó la necesidad de una capacitación adicional en el tema de la construcción de indicadores resumen estandarizados (razones, proporciones y tasas) y su interpretación en cada caso, a fin de que su trabajo no se convierta en una mera rutina «intrascendente de llenado de formularios».

— Otro aspecto de suma importancia, que pone en riesgo el flujo normal y continuo de la información que se genera, es la alta movilidad de funcionarios encargados de estas tareas técnicas, que en muchos casos a tiempo de haber adquirido alguna experiencia por iniciativa propia en el llenado de los formularios son reemplazados por personal nuevo y sin el perfil profesional requerido.

— También se pudo percibir que la falta oportuna y disponibilidad de los formularios de recolección retrasa los cronogramas de reportes periódicos, aunque con el fotocopiado de los mismos se suelen superar los retrasos. En este mismo tema, se pudo advertir que por cumplir con los reportes de trabajo acumulado por la falta de formularios, se corre con el riesgo de perder calidad y precisión en el registro rápido de los datos.

— En el tema de la calidad de los datos y los resultados estadísticos centralizados, se hace necesario supervisar y evaluar el proceso continuo de la producción estadística, desde la captura, la centralización, el procesamiento hasta su difusión a fin de hacer los ajustes y correcciones oportunas y garantizar resultados finales depurados y confiables.

— Un hecho que amerita tomar debida nota, es que casi todos los funcionarios manifiestan no recibir la información procesada de retorno (cuadros estadísticos e indicadores) como producto de su

trabajo, lo que en cierto modo desmotiva el cumplimiento eficiente de sus funciones.

— Por otra parte, de acuerdo a los resultados del primer momento del ciclo de información, se pudo observar una diversidad de registros de sistematización, entre los que se puede mencionar: el Libro del Programa Ampliado de Inmunizaciones (PAI), el Cuaderno de Salud Reproductiva, el Libro de Atención Prenatal, el Cuaderno de Consulta Externa, el Cuaderno de Tuberculosis y otros instrumentos que conforman el conjunto total de registro del sector, cuyo llenado lleva mucho tiempo, «descuidando la atención médica de los pacientes que acuden al centro de salud». Este hecho hace suponer la falta o escasez de personal destinado a estas tareas, principalmente en los establecimientos del área rural.

— El uso de los registros de sistematización no siempre es el correcto; un ejemplo concreto es el caso del «Cuaderno del Programa Ampliado de Inmunizaciones» (PAI), los mismos que en algunos establecimientos no son llenados durante las campañas de vacunación, más por el contrario y de manera indebida, lo hacen en otros cuadernos. En otros casos el registro es incompleto, lo que induce a una omisión de datos. Esta situación puede ocasionar, problemas en términos de calidad y completitud de la información.

— Por esta razón, el esfuerzo estará dirigido a contar con formularios y registros estándar en los servicios de salud y con el personal adecuado, con el fin de facilitar el registro y la sistematización de todos los datos de las variables incluidas en el SNIS y evitar su dispersión, lo que ayuda al trabajo de trascripción en todos los niveles y contribuye a una buena supervisión, un mejor control de calidad y análisis de la información.

— Otro detalle importante es el hecho de que el registro de los datos, en el ámbito de los establecimientos de salud, es realizado casi en su totalidad por el auxiliar de enfermería y por el médico en aquellos centros donde existe este recurso humano.

— El traspaso de los datos de los registros de captación a los de sistematización es ejecutado siguiendo las pautas elaboradas por el SNIS y por algunas ONG en sus áreas de influencia, para su procesamiento manual (llenado de formularios y centraliza-

ción) y electrónico para la salida de cuadros estadísticos según el plan básico de tabulados.

— También se ha detectado una demanda para desarrollar un programa de capacitación continuo al personal del sector salud en el manejo, análisis y construcción de indicadores, así como también en los determinantes de la salud (educación y vivienda, servicios básicos y medio ambiente), con una metodología adecuada y con un fuerte componente en la parte práctica y particularmente en el llenado de los formularios de captura de datos básicos y su reporte oportuno al nivel inmediato superior en la estructura. Este proceso de capacitación debe incluir aspectos de control de calidad de la información durante el proceso y además en el uso para la planificación del desarrollo y toma de decisiones.

— Otro aspecto importante es la falta de permanencia del personal médico y de enfermería en el establecimiento de salud, particularmente en el área rural donde los profesionales nuevos realizan su año de provincia y luego son promovidos o sustituidos con un personal con menos conocimiento sobre la organización y funcionamiento del SNIS; es decir, que el personal que adquirió experiencia en el sistema, «frecuentemente», es sustituido por otro, que debe seguir nuevamente su proceso de adecuación y adiestramiento en sus funciones, retrasando y desfasando los cronogramas de entrega de resultados estadísticos.

— El llenado de los instrumentos de sistematización lleva mucho tiempo por lo extenso que es en su contenido. Existen muchos instrumentos (Cuadernos, formularios e instructivos). Se sugiere estudiar la forma de reducir a lo estrictamente necesario para los fines del Ministerio de Salud.

— Los problemas más agudos en el llenado de los formularios se presentan en los centros de salud del área rural, donde se «pasa mucho tiempo llenando los formularios» (centros de salud y domiciliario), descuidando otras actividades en materia de atención de salud a los pacientes.

— Otro problema es el de las distancias entre el establecimiento de salud y la gerencia de red, dificultando la comunicación, lo que muchas veces retrasa la entrega oportuna de los reportes mensuales y semanales. Esta debilidad se puede superar llegando con el flujo de información hasta los establecimientos o centros de

salud con una red de comunicación electrónica que cubra todo el territorio nacional, además equipando con computadoras de última generación a los responsables de estas tareas (Ayala, 2013).

2.6.13 DETERMINACIÓN DE LA CALIDAD DE LOS RECURSOS HUMANOS CON QUE CUENTA EL SISTEMA

El Sistema Nacional de Información en Salud (SNIS) dispone de recursos humanos muy heterogéneos en todos los niveles de su estructura, con un personal calificado y con el perfil adecuado en los niveles de prestación de servicios, pero con una falta notoria de un perfil requerido para el llenado de los formularios de captura de los datos básicos.

Las enfermeras auxiliares, que llenan los formularios de captura no tienen la formación académica requerida para este tipo de actividades. Tienen una formación muy inicial y el logro de un conocimiento en estas tareas es a base de una iniciativa y esfuerzo personal de una interpretación y estudio de los instructivos. Por esta razón y a fin de estandarizar los criterios del llenado de los formularios, se requiere programar una capacitación teórica y práctica a este personal tan importante en el inicio del ciclo de la información en salud.

Sin embargo, se ha podido advertir una alta predisposición por cumplir sus funciones según el cargo que les ha asignado según el manual de funciones del sistema (Ayala, 2013).

2.6.14 USO DE LA INFORMACIÓN DE SALUD

La información generada por el SNIS tiene como objetivo principal, satisfacer las demandas de usuarios internos y externos del sistema. Los usuarios internos del propio sistema utilizan la información para la evaluación de resultados finales, ajustes de datos de las series cronológicas y como retroalimentación a los procesos continuos de elaboración de información.

El Ministerio de Salud usa la información para la elaboración del escudo epidemiológico del país y de los nueve (9) Departamentos del país, para la elaboración de los Planes Operativos Anuales (POA) y Planes Operativos Anuales Individuales (POAI), para el seguimiento y

evaluación de los programas ejecutados y en ejecución. En suma, la información que proporciona el SNIS es útil para reflejar la situación y el perfil del estado de la salud del país y de sus diferentes niveles geográficos (departamentos, provincia y municipios), con la finalidad de precisar y visualizar los problemas del sector y direccionar las acciones con mayor eficiencia y tomar las decisiones más precisas.

Los usuarios externos, como el Instituto Nacional de Estadística (INE), utilizan los datos para la construcción de indicadores de salud de los diferentes eventos registrados en el SNIS y efectuar los análisis comparativos con los indicadores construidos con base a las encuestas nacionales de demografía y salud (Ministerio de Salud y Deportes, 2010).

2.6.15 DETERMINACIÓN DE LA SUFICIENCIA O INSUFICIENCIA DE LOS RECURSOS MATERIALES A LOS QUE TIENE ACCESO

Si bien el sistema cuenta con una asignación presupuestaria, la misma es lo suficiente para el cumplimiento eficiente de sus funciones. El sistema no dispone regularmente de los recursos materiales suficientes para el desempeño de sus actividades.

Los materiales y suministros no son remitidos oportunamente a los centros de salud del interior del país y especialmente a los que se encuentran en las áreas rurales.

También requiere de la dotación de equipos de computación personal más actuales o de una generación más reciente, para encarar sus actividades con mayor eficiencia y motivación. En cuanto se refiere a la infraestructura, el personal trabaja en condiciones de hacinamiento, en espacios reducidos que se traducen en una debilidad del sistema.

2.6.16 DIAGNÓSTICO GENERAL EN EL MARCO DEL SISTEMA NACIONAL DE ESTADÍSTICA

El diagnóstico detectó los problemas generales que dificultan el normal desempeño de sus funciones; estos problemas se resumen en tres componentes que son: sistema de producción, sistema de información y sistema de coordinación.

2.6.16.1 Sistema de Producción

— Ausencia de información estadística con carácter desagregado depurado y con consistencia.

— Se ha descuidado la producción de estadísticas de calidad que permitan un mejor cálculo.

— De indicadores sostenidos y consistentes.

— Existe una brecha entre la oferta y demanda de información estadística de instituciones del sector público y el privado.

— Se manifiesta una centralización administrativa de la información estadística.

— Se evidencia falta de sostenibilidad financiera para de la producción estadística.

— Se denota poca atención de instancia superiores por satisfacer la demanda presupuestaria para mejorar/reforzar las Unidades Estadísticas.

— Desfase entre la información disponible a nivel regional y nacional (Ayala, 2013).

2.6.16.2 Sistema de Información

— Hay dificultad por acceder a la información estadística por cualquier persona natural o jurídica, sea de fuente pública o privada.

— No hay apertura de medios de comunicación para difusión de la información estadística.

— Se destaca en gran parte de las publicaciones el no respetar las fuentes originales de la información estadística.

— La información estadística no está siendo socializada.

— Se denota un lenguaje muy «técnico» de las páginas web.

— La ley no está ajustada a la realidad y accesibilidad actual (proceso de difusión y concientización de la ley estadística).

— En la ley estadística no se contempla una relación estrecha con la Ley de Organización del Poder Ejecutivo (LOPE).

— Notoria deficiencia en el procedimiento de los canales de difusión.

— No hay difusión de información estadística con mayor desagregación al nivel de nacional y departamental y municipal.

— Hay constantes cambios en los equipos técnicos de comunicación institucionales.

— El estado no destina presupuesto adicional para la sostenibilidad de la producción de información estadística y difusión de medios de comunicación.

— Deficiencias en el control de difusión de la información estadística.

— No hay importancia de las instituciones en la utilización de la información estadística. (Ayala, 2013).

2.6.16.3 **Sistema de Coordinación**

— Se observa el alto volumen de producción de información estadística del sector público, sin embargo, existen dificultades en el sector privado.

— Pese a haber mejorado sustancialmente en los últimos años en materia de capacitación de recursos humanos y haber ganado confiabilidad, no logra posicionarse para cumplir el rol del Sistema.

— Debilidad por contar con cuadros de recursos humanos capacitados por la constante movilización de los mismos.

— No hay coordinación con las investigaciones estadísticas que realizan otras instituciones.

— No se cuenta con un plan mínimo para la producción de estadística que permita satisfacer la demanda insatisfecha de información estadística.

— No se comparte la información obtenida a través de investigaciones especiales de cada una de las instituciones que generan información similar.

— Falta capacitación acerca de los objetivos de cada investigación estadística.

— No se aprovecha la capacidad de las cámaras para la organización de eventos de capacitación en procura de mejorar el sistema de información estadística.

— No se vela por mejorar los mecanismos que permitan hacer llegar la información estadística a instancias como municipios pequeños que no tienen las condiciones técnicas a nivel informático (Ayala, 2013).

2.7 SISTEMAS DE INFORMACIÓN EN EL ÁMBITO SANITARIO DE BOLIVIA

Mediante Resolución Ministerial 0853 de fecha 18 de noviembre de 2005, se dispone la implementación en los establecimientos de salud de los tres niveles de gestión el Sistema de Información Gerencial «WINSIG», desarrollado por la Organización Panamericana de la Salud, el Sistema Integrado de Administración Financiera (SIAF) y el Sistema Integrado Clínico Estadístico (SICE) desarrollados por *Medicus Mundi*[13], para apoyar a las acciones que desarrolle el Sistema Nacional de Información en Salud y la Vigilancia Epidemiológica (SNIS-VE).

---

[13] Medicus Mundi-Delegación Bolivia, es la representación de Medicus Mundi España en Bolivia, Organización No Gubernamental sin fines de lucro, de apoyo al desarrollo, especializada en temas de salud, independiente tanto confesional como políticamente. Esta organización tiene una larga y amplia experiencia de cooperación en Bolivia tanto en el sector sanitario como en otros ámbitos del desarrollo. Su trabajo se remonta a 1998, año en el que empieza a ejecutar el Proyecto Salud Norte de Potosí. A partir de los años 90, esta cooperación va ampliándose con nuevos proyectos y nuevas zonas de intervención gracias a la contribución de múltiples financiadores: Agencia Española de Cooperación Internacional, Comisión Europea, Gobierno de Navarra, Gobierno Vasco, entre otros.

El Ministerio de Salud y Deportes como ente normativo nacional aprueba como instrumentos oficiales el software WINSIG, SIAF y SICE, los mismos que deben implementarse gradualmente en los establecimientos de segundo y tercer nivel (artículo 1, Resolución Ministerial 0853).

El Sistema Nacional de Información en Salud a nivel nacional y departamental coordinará con las organizaciones de apoyo internacional para la transferencia de tecnología, instalación y capacitación en los establecimientos de salud que cuenten con los recursos físicos y humanos asignados para el funcionamiento de estos subsistemas como parte del SNIS en uso de sus atribuciones y responsabilidades será el encargado de dar cumplimiento a lo dispuesto en la Resolución Ministerial 0853 (artículo 2, Resolución Ministerial 0853).

2.7.1 SISTEMA INTEGRADO DE ADMINISTRACIÓN FINANCIERA

El Sistema Integrado de Administración Financiera (SIAF) es diseñado para la Administración de Hospitales Bolivianos.

Permite crear una base de información integrada y confiable para la toma de decisiones de la Dirección Hospitalaria, favoreciendo la planificación, ejecución y control. Mejora el control administrativo y financiero de los recursos hospitalarios. Favorece el cumplimiento de normas y leyes bolivianas que regulan el funcionamiento de los sistemas administrativos de las entidades públicas.

Entre sus características están que es un Sistema Informático Integrado cuyo centro es el módulo contable presupuestario, de tal forma que el resto de los procesos administrativos generan automáticamente un movimiento en el citado módulo. Es un sistema multiusuario, en red, con niveles de seguridad que controlan las terminales de acceso al sistema, los usuarios y archivos internos de control y auditoria (Medicus Mundi, 2006).

Es un sistema informático hecho en Bolivia, por bolivianos conocedores del sistema de salud de Bolivia y que puede ser adaptado y complementado a la realidad de cualquier centro hospitalario. Está

diseñado en base a los conceptos universales de administración financiera y a la normativa legal boliviana (Ley del Sistema de Administración Financiera y Control Gubernamental, Ley de Participación Popular, Ley de Descentralización Administrativa, entre otras).

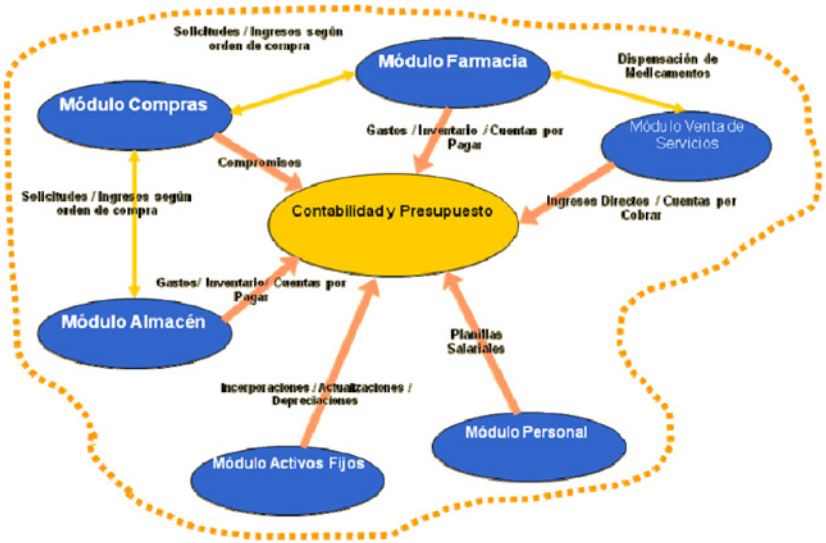

Figura 9. Sistema Integrado de Administración Financiera

Fuente de elaboración: Sistema Nacional de Información en Salud.

El SIAF es un Sistema Integrado de Administración Financiera diseñado para la Administración de Hospitales Bolivianos que tiene como objetivo trabajar e integrar los procesos administrativos y financieros de un establecimiento de salud, de modo que la información se pueda procesar de forma automática, confiable y oportuna pueda apoyar a la administración, planificación, análisis y toma de decisiones preferentemente en los hospitales del sector público.

El Sistema de Información Integrado de Administración Financiera (SIAF) al ser un sistema de información integral interactúa con módulos para su buen funcionamiento y desarrollo ya que la información contenida en cada uno de los módulos se integra en la parte de contabilidad.

La parte contable y presupuestaria del Hospital permite definir objetivos y metas expresados en unidades financieras cuyo resultado será:

a) Generar comprobantes automáticos desde los demás módulos.

b) Realizar la ejecución presupuestaria de manera automática.

c) Controlar el gasto en base a la planificación presupuestaria evitando sobregiros y déficits.

d) Reformular el presupuesto.

e) Realizar cierre de gestión de manera automática.

Este sistema integral además permite la administración de farmacias, almacenes, activos fijos, recursos humanos y contabilidad. Los módulos de interacción del Sistema Integrado de Administración Financiera (SIAF) son:

— *Módulo de Almacén:* que está encargado de registrar la información física y financiera de las compras de materiales y suministros del hospital, lo que permite mantener un Kardex valorado automático, controlar el consumo por servicio y por responsable, manejo de solicitudes y el manejo de inventario.

— *Módulo de Compra:* este módulo registra la información del proceso de compras y licitaciones y permite realizar las solicitudes de compra de farmacia, almacenes o servicios, emite las solicitudes de cotizaciones, registra las cotizaciones, registra las adjudicaciones. Asimismo, está integrado con los Módulos de Farmacia y Almacenes porque los productos adjudicados automáticamente se registran en los inventarios de farmacia o almacenes.

— *Módulo de Farmacias:* está encargado de registrar todos los movimientos físicos y financieros de la administración de la farmacia del hospital que permite mantener un Kardex valorado y automático, controlar las fechas de vencimiento, ventas de medicamentos, manejo de inventario, emitir reportes adecuados al Sistema Nacional Integrado de Salud (SNIS). Manejo de datos de medicamentos adecuados a las normas, por ejemplo, la forma farmacéutica, la concentración y finalmente el envío de archivo de los municipios en el sistema SICOFS.

— *Módulo personal:* este módulo registra la información de los recursos humanos con los que cuenta el hospital, el mismo permite registrar las planillas de sueldos, adecuadas a las normas vigentes, controlar la asistencia de manera automática a través de tarjetas magnéticas y tener información de los recursos humanos tales como formación, cursos de capacitación, memorandos y permisos.

— *Módulo de Activos Fijos:* es aquel que controla el inventario de Activos Fijos del Hospital que permite registrar altas, bajas y transferencias de estos bienes. Además de calcular depreciaciones y actualizaciones de acuerdo a normas vigentes y determina el activo fijo de forma global y por diferentes criterios: fecha, responsable, rubro y ubicación.

2.7.2 SISTEMA DE INFORMACIÓN CLÍNICO ESTADÍSTICO

El Sistema de Información Clínico Estadístico (SICE), también desarrollado por *Medicus Mundi*, permite capturar información de las historias clínicas, generando información importante para el desarrollo de investigaciones médicas y sociales.

El SICE es un sistema que registra la información clínica detallada de los pacientes. A partir del registro detallado por paciente, es posible construir los reportes que se requieran, evitando un doble registro y esfuerzo en un procesamiento adicional de datos (Medicus Mundi, 2006).

El SICE es un Sistema de información Integrado Clínico Estadístico cuyo objetivo principal es integrar en un solo lugar todos los registros médicos de un establecimiento de salud.

Los objetivos secundarios del SICE son:

— Organizar, revisar, mantener al día, archivar y custodiar los registros médicos y otros documentos hospitalarios de acuerdo a las normas establecidas.

— Convertirse en una herramienta informática que permita administrar de manera óptima el Archivo de HC.

— Recolectar, procesar y presentar la información estadística hospitalaria necesaria.

— Apoyar a los estudios de investigación desarrollados por otras áreas del hospital.

— Brindar facilidades para realizar estudios de investigación.

— Brindar facilidades de análisis a los niveles gerenciales (dirección, planificación, comités de asesoramiento, etc.)

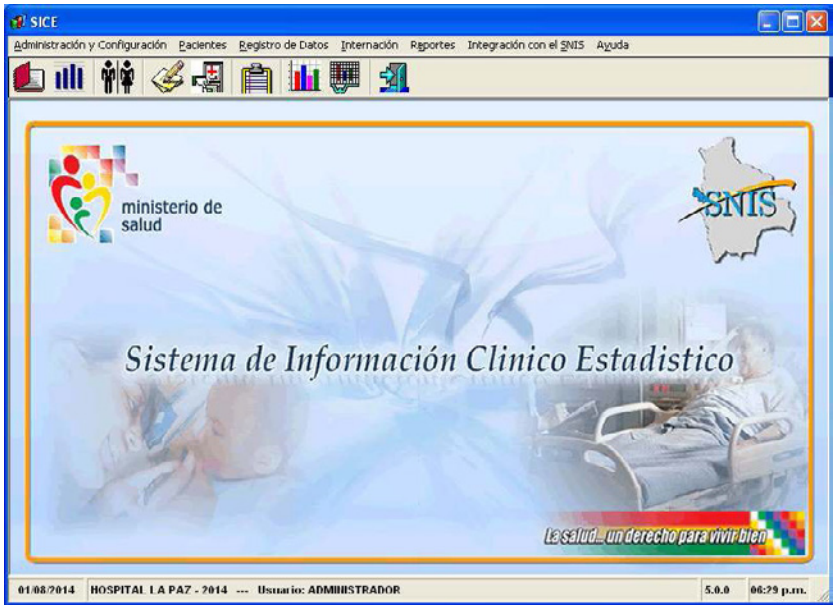

Figura 10. Sistema de Información Clínico Estadístico

El SICE es un instrumento informático de uso administrativo y operativo, pero puede servir como instrumento gerencial a través de sus reportes y su módulo de análisis de información. Por lo tanto, el uso concierne en primera instancia a quienes tienen la responsabilidad de registrar la información clínica y estadística; en segundo lugar, concierne al departamento de estadística del establecimiento que debe validar la información y finalmente concierne a los niveles de decisión del establecimiento que usarán los reportes emitidos por el módulo.

Los procesos principales que apoya son:

— Admisión de Consulta Externa.

— Admisión Hospitalaria.

— Archivo Clínico.

— Registro de Consulta Externa desde el servicio de consulta externa y/o en estadística.

— Registro de Emergencias en el servicio de Emergencia o desde estadística.

— Internaciones y Altas hospitalarias.

— Servicios auxiliares como Rayos X, Ecografía, Laboratorio, Mamografía, Nutrición, etc. (se puede configurar para que soporte otros servicios auxiliares y de apoyo al diagnóstico).

— Registro de Hechos Vitales.

— Impresión y Generación de formularios de consolidación definidos por el SNIS.

— Envío de información de Hechos vitales al sistema SIAHV.

— Generación de archivo desagregado atención por atención a plataforma web de consolidación del SNIS-VE.

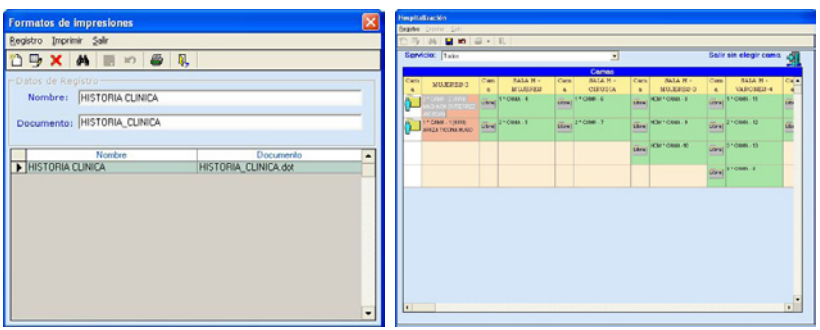

Figura 11. Vistas del Sistema de Información Clínico Estadístico

Fuente de elaboración: Sistema Nacional de Información en Salud.

Con el SICE se logra que la información clínica y estadística se registre en un solo lugar y esté almacenada para que pueda ser usada por el establecimiento, uno de los principales problemas de la información clínica y estadística es que se utilizan muchos tipos de registros y cada registro es solo propiedad del servicio que lo llena, evitando así que la información sea útil a toda la institución.

— Con la implementación del SICE se obliga a estandarizar los registros médicos.

— Con la implementación del SICE se obliga a revisar todo el flujo de información de estadística y su procesamiento de datos.

— Con la implementación del SICE se obliga a organizar el archivo clínico.

— Con la implementación del SICE se obliga a revisar los flujos de información e instrumentos de registro de consulta externa, hospitalización, emergencias y servicios auxiliares.

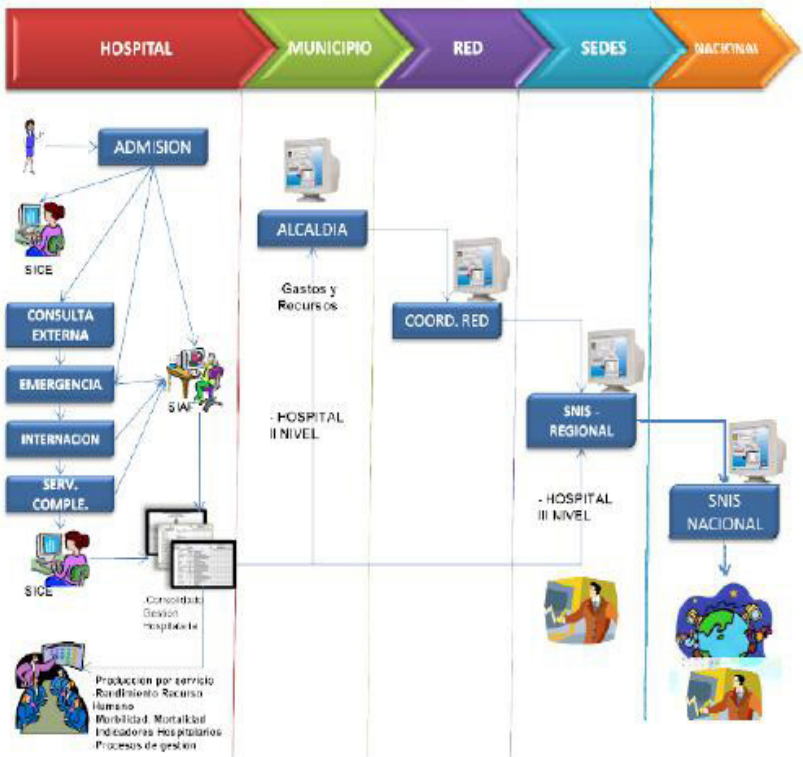

Figura 12. Estructura de la recogida de la información del SICE

Fuente de elaboración: Sistema Nacional de Información en Salud.

El sistema permite tener la información clínica y estadística del establecimiento en línea, por ejemplo, en el momento en que laboratorio emita y registre el resultado de un análisis, el médico de consulta externa puede ingresar desde su consultorio a dicho análisis.

La versión que se utiliza actualmente es la versión 501 donde se puede ver cómo crear la internación y todas las opciones, reportes y temas básicos de cómo operar el sistema.

Lo que SNIS hace es estandarizar procesos, definir qué formatos de información se van a llenar, basados en los procesos de sistematización, no pensado en una historia clínica digital sino en procesos estadísticos con el objetivo de generar información estadística para niveles operativos como niveles subnacionales. El proceso de sistematizar la información estadística empieza en las partes diarias, en conjunto externo, en el registro de internaciones; lo que hace el SICE es sistematizarlo, es decir, que se pueda traducir en una pantalla digital, en una hoja electrónica para luego ser almacenado en una base de datos partiendo de la información del paciente.

En los hospitales no funcionan los cuadernos como lo hacen en los centros de salud; lo más factible para gestionar información son las hojas de registro diario. Lo que hacen los sistemas es respaldar eso; tecnológicamente responden a esos formularios.

Hay dos (2) procesos que se están implementando en los hospitales y dependen de la infraestructura computacional con la que cuentan: Si el hospital cuenta con computadoras para sus médicos, se implementa los sistemas (SIAF, SICE, otros). Si el médico no tiene computadora, entonces se parte del proceso de transcripción de formulario, en estadística llamado el «procesamiento de información» porque no solamente se transcribe sino también se codifica, a los códigos a nivel internacionales CIE-10. Dentro de esas instancias, el médico no está capacitado para codificar, lo que implementa el SICE en los hospitales es el proceso de consulta externa donde se incorporan variables como el diagnóstico descriptivo donde se da la libertad a que el médico pueda colocar libremente lo que percibe. Posteriormente se ingresa a una plataforma donde el médico ingresa las variables solicitadas.

El proceso de sistema dentro de un hospital se divide en dos (2), dependiendo el ciclo y el circuito que tenga el mismo. Cuando se busca algún dato del paciente, se cargan todos sus datos: estado civil, edad,

ocupación, lugar de nacimiento o valores de interculturalidad; este último, referido al idioma y se lo pide más en hospitales de primer nivel. La interculturalidad va muy relacionada con el manejo de identificación de los grupos poblacionales que son atendidos por el Sistema de Salud.

Lo que se trata de ver con este sistema es la transitabilidad de los pacientes, pensando en establecer un Centro Integral fortalecido que tenga varias especialidades o fortalecer el hospital existente, para eso sirven las variables del lugar de nacimiento, donde vive, etc. El SNIS responde a la necesidad de los normadores, en Bolivia el Ministerio de Salud es el normador, ellos indican qué se debe utilizar. Sin embargo, la parte técnica médica indica las variables que se deben incorporar.

En estos últimos años se ha visto mucho el paralelismo de la información, la fragmentación del sistema, cada unidad vela por su interés, por sus propios sistemas de información, a veces no son necesariamente software, sino hojas electrónicas, correos electrónicos; una forma de transmitir información.

En temas de seguridad, la información, la integridad y la confiabilidad que tenga el dato, al estar en un Sistema de Información basado en un software, se tiene la seguridad de que está en una base de datos, misma que está distribuida en 3.746 establecimientos, entre ellos se encuentran los siguientes:

Tabla 4. Establecimientos de salud del SNS de Bolivia

Fuerzas Armadas	7
Iglesia	89
Organismos Privados	205
ONG	125
Policía Nacional	6
Público 3104	3.104
Seguridad Social	210
TOTAL	**3.746**

Fuente de elaboración: Sistema Nacional de Información en Salud.

Todos estos centros reportan información al SNIS, en las clínicas privadas cuando SEDES da su autorización para funcionar debería también pedir información, porque SEDES es quien autoriza el funcionamiento de las clínicas.

2.7.3 SOFTWARE DE ATENCIÓN PRIMARIA EN SALUD

El Software de Atención Primaria en Salud (SOAPS) se constituye en la principal herramienta tecnológica de apoyo a la gestión de la información de producción de servicios en los establecimientos salud de primer nivel de atención y modelo de integración de SNIS-VE en el marco del sistema único de información en salud, identificando como punto de encuentro de unificación los procesos de sistematización de la información (cuadernos), el mismo está desarrollado a partir de los datos de producción de servicios y su vinculación a las herramientas instituidas por los seguros públicos permitiendo obtener información desagregada desde el nivel de su obtención hasta el nivel nacional, respecto a prestaciones, manejo de medicamentos de acuerdo a la norma del SNUS, así como la inclusión de datos antropométricos.

Figura 13. Software de Atención Primaria en Salud

Fuente de elaboración: Sistema Nacional de Información en Salud.

La aplicación del Software de Atención Primaria en Salud (SOAPS) prescinde definitivamente de la utilización de los cuadernos en los establecimientos, reduciendo al personal de salud del tiempo requerido para el llenado de estos registros administrativos; punto de inflexión para la automatización de los procesos de gestión de la información desde su sistematización en adelante.

La información digital generada por dicho sistema debe ser transferida al nivel subsiguiente de dos formas: *Agregada*, por la cual los archivos de transferencia de los instrumentos consolidadores generados en el establecimiento de salud son enviados a la coordinación de servicios de salud y sucesivamente al nivel superior, respetando los mismos tiempos de la aplicación del modelo manual, y *Desagregada,* mediante el envío directo del archivo de transferencia al SNIS-VE nacional a través de un sitio web desde el mismo establecimiento de salud, siempre y cuando se cuente con servicios de internet o en su defecto desde la coordinación de servicios de salud correspondiente, de esta manera el SNIS-VE departamental, la red de servicios de salud, como la red municipal podrán tener acceso a esta información vía web (Ministerio de Salud y Deportes, 2012).

Como antecedente al Software de Atención Primaria en Salud (SOAPS), se puede mencionar que en el año 2008 el Sistema Nacional de Información en Salud (SNIS) administraba la información a través de dos (2) consolidadores que son la Información de Producción de Servicios y la Información de Vigilancia Epidemiológica; mediante este sistema se podía recuperar toda la información de manera mensual.

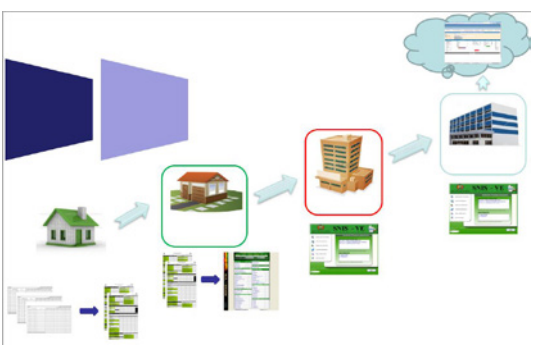

Figura 14. Modelo manual de consolidación de información

Fuente de elaboración: Sistema Nacional de Información en Salud.

Cada establecimiento de salud cuenta con cuadernos generados por el SNIS, los cuales son elaborados en base a los programas del Ministerio de Salud, como ser: cuaderno de consulta externa, cuaderno de mujeres en estado de gestación, cuaderno de atención integral del menor de 5 años, cuaderno de anticoncepción, cuaderno de internación, cuaderno de odontología, cuaderno de actividades del establecimiento de salud con la comunidad, etc.

El SNIS es quien determina las variables que tendrán todos los cuadernos y cuales se consolidarán para el informe mensual. El SNIS hace imprimir esos cuadernos y son llevados a todos los establecimientos de salud de Primer Nivel para que se puedan registrar las variables solicitadas, después esta información es desagregada por género y grupo etario.

El tiempo que se tiene para el llenado de estos cuadernos, por norma, es de quince (15) minutos por paciente, mediante tiqueos en los formularios. Para el llenado de estos cuadernos, existe una capacitación destinada al personal de salud; también se elaboran instructivos mediante el Servicio Departamental de Salud (SEDES).

Estos cuadernos son firmados por los médicos atienden a los pacientes y tienen valor de Declaración Jurada. El cuaderno no es una Historia Clínica, es un sistematizador. De todos estos cuadernos, se elaboró el Software de Atención Primaria en Salud (SOAPS).

En el SOAPS se tienen los mismos cuadernos con las mismas variables. Mediante el computador se van llenando las variables solicitadas por el software que automáticamente genera los indicadores.

Todavía los establecimientos de salud del área rural no cuentan con este software y aún llenan los cuadernos de manera manual, ello porque no cuentan con la infraestructura tecnológica necesaria. Actualmente el 65% de todos los establecimientos de salud están utilizando el sistema. Un 35% aún realiza el llenado de los cuadernos de forma manual. En el sitio web www.consolidacion.minsalud.gob.bo, se puede revisar la cantidad de establecimientos de salud que cuentan con el sistema.

Existen aproximadamente ciento nueve (109) redes en los nueve (9) departamentos y cada Red tiene una cantidad de Municipios a su cargo; las redes están administradas por los Gobiernos Autónomos Departamentales.

Mediante la Resolución Ministerial 1707 de fecha 5 de diciembre de 2014 se pide que se consolide la utilización de los sistemas dentro de los servicios de salud y exige que cada Gobernación impulse la implementación de estos en todos los establecimientos de salud a su cargo.

Todo el sistema de consolidación pretende tener datos de morbilidad de las personas dentro del territorio nacional. Existe un aproximado de 25% de error debido a la transcripción de los datos por lo que existe un 75% de confiabilidad.

Una de las grandes ventajas en la utilización de estos sistemas es que todo es automático y la información está disponible en red. Mediante un sistema de monitoreo se puede supervisar y contar con información de manera rápida y oportuna. Cuando la información no llega oportunamente se sanciona con una llamada de atención o un memorándum de incumplimiento.

El procedimiento de llenado de los cuadernos de forma manual es el siguiente: Cada establecimiento de salud debe consolidar su información hasta el 5 de cada mes, después cada Coordinador de Red lo hace hasta el 10 de cada mes, luego el SEDES hace un control de calidad hasta el día 18 del mes y finalmente el Ministerio de Salud tiene la información publicada hasta el 30 de cada mes.

Lo que se pretende con la implementación de los sistemas es que haya una consolidación de la información en los establecimientos de salud hasta el 5 de cada mes y luego automáticamente se generen los reportes para el Coordinador de Red, el SEDES y el Ministerio de Salud. De esta manera se rompe la dependencia de instancias previas para poder manejar la información, además de obtener información rápida, oportuna y con menos cantidad de errores.

Se da el margen para consolidar la información hasta el 5 de cada mes porque aún no todos los establecimientos de salud están conectados al internet. El sistema está diseñado para que se pueda ingresar los registros de forma diaria, semanal o mensual.

El SNIS solamente recoge información de los establecimientos de salud pública y seguridad social a corto plazo, lamentablemente no solicita información de los establecimientos de salud privados y organismos con o sin fines de lucro.

La Contraloría General del Estado realizó una auditoría informática a los sistemas del SNIS, la cual recomendó que el sistema debiera

abarcar a todos los establecimientos de salud independientemente de su clasificación. Al Ministerio de Salud se le otorgó un plazo de tres (3) años para que pueda cumplir con esta recomendación (Bustillos, 2015).

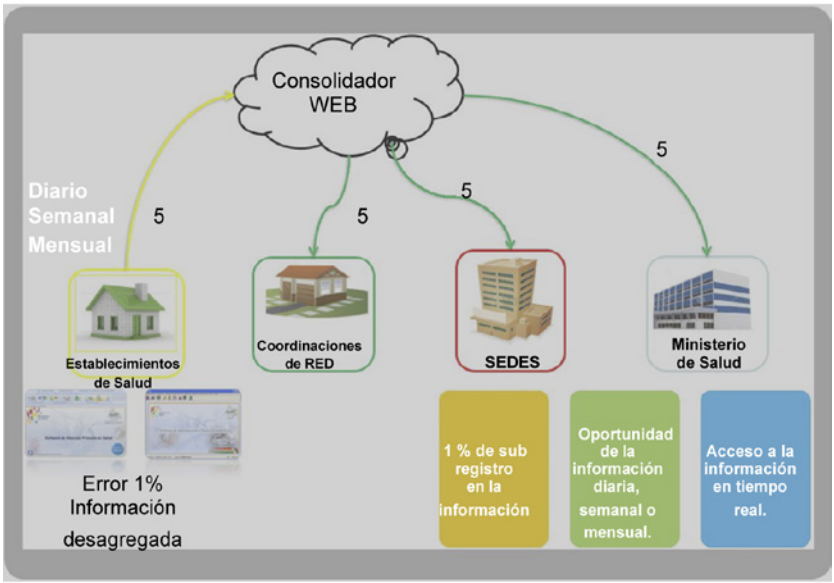

Figura 15. Qué hemos logrado con la implementación de los sistemas
Fuente de elaboración: Sistema Nacional de Información en Salud.

2.8 TELESALUD: TECNOLOGÍA EN SALUD PARA LOS BOLIVIANOS

2.8.1 ANTECEDENTES

Este proyecto nace bajo la decisión del Gobierno Nacional que incorpora, en aras de la revolución sanitaria en Bolivia, el *Proyecto de Telesalud* que busca reducir la exclusión social, promoviendo alternativas adecuadas para mejorar el acceso a la salud, superando barreras en tiempo y espacio.

El Proyecto de Telesalud implementado en Bolivia está enfocado al uso de tecnologías avanzadas que sirven para intercambiar información médica y proveer servicio médico a distancia.

A través de esta tecnología, más de 2.500 médicos denominados «Mi Salud» distribuidos en distintos municipios del País logran una conexión con hospitales de Tercer Nivel intercambiando información sobre las enfermedades de sus pacientes. Además, Telesalud permite que un paciente que necesita de manera urgente atención médica pueda ser atendido por un especialista a distancia gracias a este nuevo sistema (Mi Salud, 2014).

2.8.2 MARCO LEGAL

Telesalud para Bolivia es un proyecto que se encuentra dentro del marco legal de la Constitución Política del Estado, que en los parágrafos I y II del artículo 18 establece que «toda persona tiene derecho a la salud, así también prevé que el Estado garantiza la inclusión y el acceso a la salud de todas las personas, sin exclusión ni discriminación alguna». Además el parágrafo I del artículo 35 dispone que «el estado proteja el derecho a la salud, promoviendo políticas públicas orientadas a mejorar la calidad de vida, el bienestar colectivo y el acceso gratuito de la población a los servicios de salud».

Asimismo, la Ley de Modificaciones al Presupuesto General del Estado 396 de fecha 26 de agosto de 2015, en el artículo 21 señala:

> Artículo 21.° (Financiamiento para el proyecto «Telesalud para Bolivia»)
>
> I. «En el marco de la política de Salud Familiar Comunitaria Intercultural (SAFCI), se autoriza al Ministerio de Salud y Deportes implementar la primera fase del proyecto «Telesalud para Bolivia» a nivel nacional.
>
> II. A efecto de dar cumplimiento al parágrafo precedente, se autoriza al Ministerio de Economía y Finanzas Públicas, a través del Tesoro General de la Nación, asignar hasta Bs.139.200.000.-(Ciento Treinta y Nueve Millones Doscientos mil 00/100 Bolivianos) a favor del Ministerio de Salud y Deportes; para lo cual los Ministerios de Economía y Finanzas Públicas y de Planificación del Desarrollo, en el marco de sus competencias, deberán efectuar los traspasos presupuestarios correspondientes, que incluye consultorías.
>
> III. El Ministerio de Salud y Deportes es responsable de la ejecución, seguimiento y evaluación del proyecto «Telesalud para Bolivia», así como del uso y destino de los recursos asignados en el presente artículo»

En cuanto a la Ley 031 de Autonomías y Descentralización «Andrés Ibáñez» de fecha 19 de julio de 2010, en el numeral 4 del parágrafo I del artículo 18 define que el Ministerio de Salud y Deportes debe: «Ejercer la rectoría del Sistema Único de Salud en todo el territorio nacional, con las características que la Constitución Política del Estado

establece, de acuerdo a la concepción del vivir bien y el modelo de salud familiar comunitario intercultural y con identidad de género» y en el numeral 9 señala que debe: «Desarrollar programas nacionales de prevención… y gestionar el financiamiento de programas epidemiológicos nacionales…»

El Decreto Supremo 29272 de fecha 12 de diciembre de 2007, en el inciso f) del artículo 5 (Lineamientos Estratégicos) establece: «En el marco de la Política de Salud Familiar Comunitaria Intercultural, el Ministerio de Salud y Deportes prevé mejorar la extensión de coberturas y el lograr el fortalecimiento de redes de Salud, el proyecto Telesalud se constituirá en un brazo tecnológico importante en estos componentes».

2.8.3 OBJETIVO PRINCIPAL

El objetivo principal del Proyecto Telesalud para Bolivia es mejorar la calidad de la atención en salud, en oportunidad y efectividad, en el subsector público de salud, acortando las distancias que surgen a consecuencia de la barrera geográfica y la escasez de recursos humanos especializados y cuyo efecto directo se reflejará en la reducción de la morbilidad. Así también busca el fortalecimiento del Sistema de Salud de Bolivia a través de la implementación de tecnologías de información y comunicación (TIC) para el acceso oportuno de la atención médica.

Los objetivos específicos del Proyecto son los siguientes:

a) Mejorar la cobertura en la atención de la salud, a partir de la inclusión de las tecnologías de información y comunicación.

b) Fortalecer la capacidad resolutiva en los establecimientos de salud.

c) Fortalecer el trabajo de campo del personal de salud.

d) Mejorar la vigilancia epidemiológica.

e) Optimizar la gestión de información en salud.

El Proyecto de Telesalud está en proceso de implementación, capacitación y servicio de red, ejecutado interconsulta en tiempo real y diferido con el servicio de conectividad de microondas, fibra óptica y por satélite (Ministerio de Salud, 2015).

2.8.4 COMPONENTES DE TELESALUD

Los componentes de este Proyecto son:

— *Tele epidemiológica:* con información dinámica y respuesta inmediata.

— *Tele gerencia:* con el monitoreo de abastecimiento de insumos y asesoramiento técnico permanente. Digitalizar el historial clínico[14].

— *Tele educación:* con capacitación de recursos humanos y telemedicina con asistencia médica especializada virtual programada de pacientes.

— *Tele medicina:* asistencia médica especializada en tiempo real y diferido (interconsulta). Referencia programada de pacientes (Mi Salud, 2014).

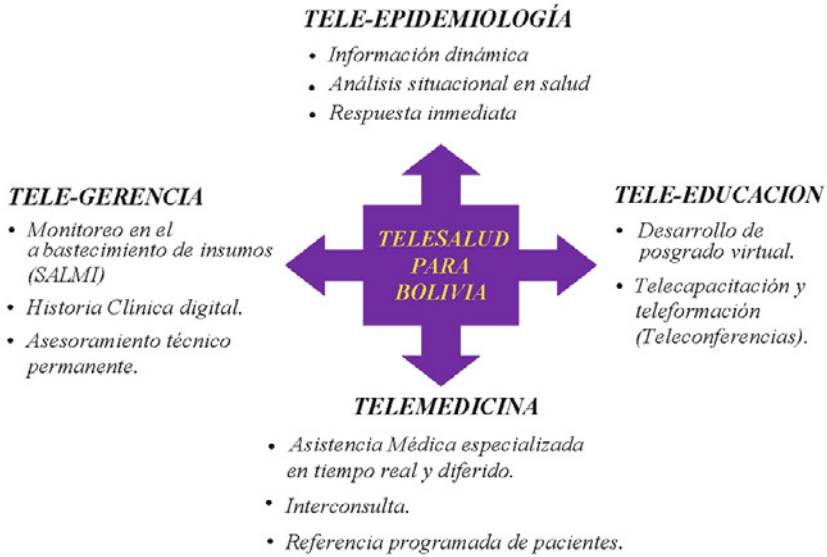

Figura 16. Componentes de Telesalud para Bolivia

Fuente de elaboración: Proyecto de Telesalud.

---

[14] El Ministro de Salud, Dr. Juan Carlos Calvimontes, anunció que para el 2015 se preparará una ley que instruya la digitalización de los historiales médicos de los pacientes. Mi Salud (2014), *«Telesalud. La tecnología al servicio de la salud»* Revista Mensual año 1/n.º 4 2014, Ministerio de Salud, La Paz-Bolivia.

2.8.5 CARACTERÍSTICAS DE LOS NIVELES DE TELESALUD

La característica principal del Proyecto Telesalud es la transformación de datos médicos en tecnología avanzada, los enlaces que se realizan en tiempo real y diferido, el manejo de historias clínicas digitales que coadyuvarán en el registro de una base de datos a nivel nacional.

Telesalud se desarrolla a través del siguiente funcionamiento:

— *TELE 1:* Son aquellos que están ubicados en los Municipios alejados y desde donde se realizan consultas médicas. Están ubicados en 269 municipios disponiendo de equipamiento médico y portal de videoconferencias acorde al nivel de complejidad. Los dispositivos médicos son: cámara de examen, otoscopio, electrocardiograma, monitor de signos vitales, equipo de ultrasonido y cámara para videoconferencia.

— *TELE 2:* Están ubicados en los hospitales de Segundo Nivel, están en conexión con los Tele 1 y los Tele 3. Se conectarán en 62 municipios, disponiendo de equipamiento médico y portal de videoconferencia, acorde a los niveles de complejidad. Los dispositivos médicos son: cámara de examen general, otoscopio, monitoreo de signos vitales, electrocardiograma, espirómetro digital, oftalmoscopio, video colposcopio, equipo ultrasonido y cámara para videoconferencias.

— *TELE 3:* Están instalados en los hospitales de Tercer Nivel en las capitales de departamento. Sus instalaciones tiene mayor cantidad de equipamiento, mejor conexión informática; están instalados en los Hospitales de Tercer Nivel porque en ellos están concentrados los especialistas, cirujanos y otro tipo de médicos al servicio de los bolivianos.

— *TELE 4:* Está a cargo el Ministerio de Salud que es la plataforma que administra la base de datos de manera digitalizada y cuenta con dos (2) servidores, dos (2) computadoras y dos (2) monitores (Ministerio de Salud, 2015).

Figura 17. Características de Telesalud

Fuente de elaboración: Proyecto de Telesalud

2.8.6 ALCANCES

Hasta agosto de 2015, son 99 municipios (puntos) ubicados en los departamentos de Cochabamba, Santa Cruz, Tarija, Beni, La Paz y Oruro donde está funcionando el Proyecto Telesalud, con más de 5.000 interconsultas médicas, además de capacitación virtual y semipresencial para el personal del establecimiento médico. Asimismo, se han realizado interconsultas de reumatología, cardiología, medicina interna, terapia intensiva y otras especialidades, bajo el monitoreo de un médico general de un municipio alejado.

El Proyecto de Telesalud tiene proyectado finalizar su fase de implementación hasta fines de la gestión 2015, garantizando cobertura total en los 339 municipios de Bolivia, brindando consultas y asistencia médica acortando distancias (Ministerio de Salud, 2015).

CAPÍTULO III
TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO SANITARIO DE ESPAÑA

3.1 LOS DATOS PERSONALES FRENTE A LA SOCIEDAD DE LA INFORMACIÓN

La progresiva e imparable introducción en nuestras vidas de las redes digitales suscita, si cabe, una mayor inquietud de cara a la protección de los derechos de la persona. Concretamente, la convergencia entre la informática y las telecomunicaciones (la denominada telemática) introduce nuevos, desconocidos y graves riesgos que ponen en peligro la integridad de uno de los que últimamente vienen siendo denominados por la doctrina derechos fundamentales de tercera generación, el derecho a la autodeterminación informativa o tutela de datos.

Esta denominación viene siendo utilizada para referirse a la facultad de toda persona a ejercer control sobre la información personal que le concierne y, en particular, sobre aquellos datos que son almacenados mediante medios informáticos. Constituye un derecho personalísimo que ha adquirido autonomía conceptual con relación a otros derechos de la persona, como la intimidad o la privacidad, la imagen, el honor o la identidad personal. Mediante su reconocimiento se persigue, en definitiva, proteger la libertad de los individuos a determinar por sí mismos, cuándo, cómo y hasta qué punto se puede comunicar a terceras personas información referida a ellos. En último término, lo que se pretende con su reconocimiento no es otra cosa que ofrecer a las personas un fuerte sistema de garantías que les asegure la tutela de otro derecho fundamental más amplio cual es el de la vida privada (Campuzano Tomé, 2000).

De lo expuesto hasta el momento se desprende que el tema de la protección de la vida privada y de los datos personales puede ser analizado desde una doble vertiente: la primera corresponde a la protección de datos personales como objeto de valor en un sistema de mercado dirigido a instaurar el comercio electrónico en cuanto principal

sistema de intercambio de bienes. En tal caso, se habla de protección a los consumidores, de protección de los datos relativos al consumo, de protección del comercio electrónico, de seguridad de las transacciones electrónicas, de nuevas formas de contratación. La otra vertiente se refiere a la protección de los datos como medio de protección de la persona dirigido a salvaguardar uno de los principales derechos fundamentales cual es el derecho a la vida privada.

Señala Campuzano Tomé (2000:65) que «las injerencias en la vida privada motivadas por la mala utilización del tratamiento de los datos informáticos, en la medida en que afectan al ámbito de la personalidad, producen efectos negativos irreparables. La violación del derecho a la vida privada no permite reparación posible». Tales intromisiones en la vida privada de los sujetos producen consecuencias gravemente perjudiciales que deberán ser tomadas en consideración para otorgar la misma protección a los datos personales con independencia de cuál haya sido el ámbito, público o privado, en el que hayan sido recopilados y tratados.

3.2 LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL 292/2000

Va a coincidir casi en el tiempo, la configuración del derecho a la protección de datos que el Tribunal Constitucional singulariza en su Sentencia 292/2000 y la que establece la Carta Europea de Derechos Fundamentales en su artículo 8. Brevemente se analizará a continuación la formulación que hace el Tribunal Constitucional Español y el contenido dado al derecho de protección de datos por la Carta Europea.

Los fundamentos jurídicos 6 y 7 de la sentencia del Tribunal Constitucional vienen íntegramente dedicados a la definición y configuración del derecho a la protección de datos personales. El fundamento jurídico 7 de la referida sentencia remarca el contenido del derecho fundamental a la protección de datos y las facultades que proporciona al individuo frente al Estado como ante el particular; a continuación se trascriben algunos de los párrafos de los citados fundamentos

jurídicos porque las propias palabras del Tribunal Constitucional son elocuentes:

«De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o a un particular. O cuáles puede éste tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y tratamiento, informático o no, de los datos personales requiere como complementos indispensables, por un lado la facultad de saber en todo momento quién dispone de esos datos personales y a qué usos los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos».

De la anterior doctrina viene a deducirse que el Tribunal Constitucional ha venido a configurar, sin ningún tipo de ambigüedad, el derecho a la protección de datos como un derecho fundamental autónomo, desarrollando hasta sus últimas consecuencias la doctrina iniciada tímidamente por el propio Tribunal Constitucional en su Sentencia 254/1993.

Este derecho fundamental no reduce su protección a los datos íntimos, sino que su objeto de protección es cualquier tipo de dato personal, traspasando su objeto a la intimidad personal, y viniendo constituido su contenido por una serie de facultades consistentes en diversos poderes que imponen a terceros deberes tales como requerir el consentimiento para la recogida y uso de los datos personales, ser informado sobre el destino y poder acceder, rectificar y cancelar los propios datos. En definitiva, el contenido del derecho a la protección de datos personales que señala el Tribunal Constitucional viene a coincidir con los principios y derechos que establece la Ley Orgánica 15/1999 (LOPD), y que deberán respetarse y atenderse en todo tratamiento de datos personales (Serrano Pérez, 2003).

El contenido del derecho fundamental a la protección de datos consiste, en resumen, en un poder de disposición y control sobre los datos personales, tanto frente al Estado como ante cualquier particular.

3.3 LA LLAMADA LIBERTAD INFORMÁTICA

Tradicionalmente la protección de los datos personales ha estado vinculada al derecho fundamental a la intimidad personal y familiar. De esta forma aparece recogido en diversas normas internacionales y nacionales que lo configuran como un derecho singular que emerge como facultad de autodeterminación de la persona frente al desarrollo de la informática y la telemática, que van a permitir la recogida masiva de datos de los individuos y su tratamiento.

Al mismo tiempo, el Tribunal Constitucional, en su labor interpretadora del artículo 18.4 de la Constitución española, «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos», ha pasado de unos pronunciamientos iniciales que lo hacían aparecer como un mero derecho de carácter instrumental, a modo de garantía y presupuesto de la protección de otros derechos, a resoluciones posteriores en las que configura como un nuevo derecho o libertad fundamental de carácter autónomo e independiente respecto del derecho a la intimidad personal y familiar, dirigido a hacer frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos. De esta forma se habla del derecho a la autodeterminación informativa y de la libertad informática como términos conceptuales que definen la verdadera naturaleza de la protección de datos personales (Sánchez-Caro y Abellán, 2004).

El Tribunal Constitucional en la Sentencia 292/2000 de 30 de noviembre (comentada precedentemente) que resolvió el recurso de inconstitucionalidad contra la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), manifestó que la garantía de la vida privada de la persona y su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada *libertad informática* es el derecho a controlar el uso de los mismos datos insertos en un programa informático.

3.4 PRINCIPIOS BÁSICOS DE LA LEY DE PROTECCIÓN DE DATOS APLICADOS AL ÁMBITO SANITARIO

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), vino a sustituir a la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter Personal (en adelante LORTAD), a la que deroga; la LOPD tiene por finalidad principal el incorporar al derecho interno español, la Directiva 95/46/CE; aunque no se diga expresamente en la ley española, por carecer ésta de exposición de motivos e incluso de un simple preámbulo.

El artículo 1 de la Ley Orgánica 15/1999 (LOPD) declara que la ley tiene por objeto garantizar y proteger los derechos y libertades fundamentales en lo concerniente al tratamiento de los datos personales y especialmente el derecho al honor e intimidad personal y familiar de las personas físicas.

Ya no se conciben las nuevas tecnologías como un peligro claro para la intimidad, de forma que deben ser sometidas o atadas para garantizar el desarrollo de los derechos individuales; sino que partiendo de la aceptación de la informática como un medio esencial para el desarrollo de la sociedad, o al menos útil, se entiende que no debe ser limitada. Por ello, se modifica el objetivo de la ley, que pasa a ser la protección del honor, la intimidad y demás derechos individuales, en cuanto puedan verse afectados por el uso de las nuevas tecnologías (Aparicio Salom, 2000).

El objeto de aplicación de la LOPD está constituido por los datos de carácter personal registrados en soporte físico, no necesariamente en ficheros automatizados, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se prevén igualmente mecanismos de protección frente a las actuaciones contrarias a la ley, que puedan ser objeto de reclamación por los interesados ante la Agencia Española de Protección de Datos, sin perjuicio de aquellos a percibir una indemnización en los casos en que el incumplimiento de la ley les hubiera originado daño o lesión en sus bienes o derechos, vía civil. La ley contiene una serie de principios básicos que determinan una correcta protección de los datos y constituyen al mismo tiempo una garantía de los ciudadanos.

Durante la presente investigación se desarrollará el contenido de la LOPD; en especial lo relacionado con el tratamiento de los datos de salud.

3.4.1 PRINCIPIO DE CALIDAD O PROPORCIONALIDAD DE LOS DATOS

Según el artículo 4 de la LOPD, es condición para que puedan recogerse datos de carácter personal el que los mismos resulten adecuados, pertinentes y no excesivos. La ley determina también que los datos deben ser exactos y puestos al día, de forma que respondan con veracidad a la situación actual del interesado, asociando su conservación a la necesidad de su tratamiento en virtud de la finalidad para la que se recabaron, ya que cuando hayan dejado de ser necesarios o pertinentes deberán ser cancelados.

Si resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados. Esto implica:

— Tener procedimientos individualizados de actualización a petición de los interesados, así como procedimientos masivos periódicos de actualización y cancelación de los datos que mantengan la información actualizada.

— Cuando se modifiquen o se supriman ficheros de datos de carácter personal, esa modificación o supresión deberá declararse de la misma forma que se declaró su creación.

Igualmente serán cancelados los datos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados. Por ejemplo, en esta categoría podrían considerarse incluidos los procesos de «expurgo» de historias clínicas definidos en el apartado tercero de la Recomendación 2/2004 de la Agencia de Protección de Datos de la Comunidad de Madrid (APDPCM, 2008).

En el ámbito sanitario conviene recordar que la historia clínica, sea manual o informatizada, tiene su razón de ser en facilitar la asistencia sanitaria al ciudadano y que, por tanto, la naturaleza de la información que se incluye en la misma ha de ser acorde con el citado objetivo, debiéndose recoger exclusivamente toda la información clínica necesaria para asegurar, bajo un criterio médico, el conocimiento veraz, exacto y

actualizado del estado de salud del paciente, por parte de los profesionales sanitarios que le atienden (Sánchez-Caro y Abellán, 2004).

Un ejemplo de lo expuesto se recoge en la Ley 41/2002 a propósito del contenido de la historia clínica, ya que la mencionada ley dispone que la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente; en concreto, regula el contenido mínimo de la historia clínica (artículo 15.2 Ley 41/2002). No obstante, esta regulación podría acarrear en el futuro algún tipo de problema interpretativo, precisamente por su consideración de contenido mínimo que podrá completarse con cualquier información que se considere trascendental para conocer el estado de salud del paciente. Ello podría dar lugar a la inclusión de datos que supusieran valoraciones subjetivas del facultativo (Puente Escobar, 2004:33).

Todo paciente tiene derecho a que quede constancia, por escrito o en soporte más adecuado, de la información obtenida en todos sus procesos asistenciales realizados por el servicio de salud, tanto en el ámbito de la Atención Primaria como de Atención Especializada. De esta forma, todo profesional que intervenga en la actividad asistencial está obligado al cumplimiento de los deberes de información y documentación clínica (artículo 2.6 Ley 41/2002). Por tanto (hay que), se debe hacer una historia clínica en todo el proceso asistencial, tanto en la urgencia, como en atención primaria, especializada u hospitalaria.

Es necesario velar por la calidad, plenitud y exactitud de la información personal allí almacenada. De hecho, el artículo 14 de la Ley 41/2002 afirma que la historia clínica debe comprender el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos en el ámbito de cada centro. Las Administraciones sanitarias deben establecer mecanismos que garanticen la exactitud y la autenticidad del contenido de la historia clínica y los cambios operados en ella (artículo 14.3). Como se ha señalado antes, los profesionales deben cooperar en el mantenimiento de una documentación secuencial y ordenada del proceso asistencial de los pacientes (APDCM, 2004).

3.4.2 PRINCIPIO DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Este principio general de información expresa, precisa e inequívoca para el tratamiento de datos personales debe ser armonizado con las exigencias del normal funcionamiento de la actividad sanitaria, de manera que no todos los actos asistenciales repetitivos o múltiples requieran la aplicación formal de este principio. Así, la existencia de un fichero de datos personales o la finalidad de la información recabada se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Es fundamental que en cualquier caso, el centro o servicio sanitario responsable del tratamiento de los datos informe a los interesados en el momento de la recogida de los mismos sobre sus derechos relativos a sus propios datos personales. En particular, en todos los impresos o formularios de recogida de datos, con independencia del soporte de los mismos (en papel, a través de Internet, etc.) debe incluirse información relativa a los derechos que asisten a los ciudadanos y dónde y cómo ejercerlos (APDCM, 2008).

Señala la Agencia de Protección de Datos de la Comunidad de Madrid (2004:30), que el cumplimiento de este principio de información podría llevarse a efecto en el momento de la entrada en el sistema sanitario bajo diferentes formas, por ejemplo, en el momento de la obtención de la Tarjeta Individual Sanitaria (TIS), pero sería de muy difícil implantación, por no decir de imposible implantación, en cada uno de los actos sanitarios que se lleven a cabo con los pacientes o usuarios y que requieran un nuevo tratamiento de datos personales; lo contrario podría burocratizar en exceso el sistema sanitario y dificultar la gestión asistencial.

En la actualidad es cada día más frecuente el uso de cámaras de vídeo o videocámaras con una función de vídeovigilancia u otras finalidades distintas. Como se recordará, «dato de carácter personal» es cualquier información concerniente a personas físicas identificadas o identificables, de modo que como la imagen (y la voz) de una persona la identifica inequívocamente es, por tanto, un dato de carácter personal. Por otra parte, dichas imágenes y/o voces, constituyen también un «fichero» a los efectos de la LOPD. De ahí que las imágenes obtenidas mediante estos medios técnicos relativos a personas consti-

tuyan datos de carácter personal y estén, por tanto, dentro del ámbito de aplicación de la legislación de protección de datos.

Igualmente deberá cumplirse con el deber de información, instalando en lugares visibles carteles informativos que avisen al ciudadano de que se le está grabando o captando imágenes con cámaras. El distintivo informativo deberá contener una mención a la finalidad para la que se recogen y/o tratan los datos, una información descriptiva de los espacios comprendidos dentro de la zona en la que se instalen los sistemas de cámaras o videocámaras, una referencia a la LOPD, una mención expresa a la identificación del responsable ante el que puedan ejercerse los derechos a que se refiere la LOPD y la indicación de la posibilidad de obtener una información más detallada solicitando la misma en un lugar expresamente señalado al efecto (APDCM, 2008).

En el ámbito sanitario debe tenerse en cuenta, además de aquellos sistemas de captación de imágenes instalados con fines de videovigilancia, aquellos otros que pueden tener una finalidad distinta, como por ejemplo la telemedicina o el seguimiento y control de los pacientes en determinadas unidades de hospitalización. Estos tratamientos de imágenes también constituyen ficheros de datos de carácter personal sometidos a la legislación vigente en materia de protección de datos. Por otra parte, no se considerará un tratamiento específico de datos personales a la captación de imágenes para su inclusión en otro fichero o tratamiento diferente (por ejemplo, la inclusión de imágenes dentro de la historia clínica de los pacientes). En este supuesto, será el tratamiento global de los datos (imágenes y resto de información) el que estará sometido a los criterios generales establecidos por la normativa de Protección de Datos.

3.4.3 PRINCIPIO DE CONSENTIMIENTO DEL INTERESADO

La norma general en materia de protección de datos es que debe obtenerse el consentimiento inequívoco del afectado para que se recojan sus datos, salvo en casos excepcionales previstos en la ley. El consentimiento puede ser revocado, siempre que exista una causa que lo justifique y siempre que no se atribuyan efectos retroactivos a dicha revocación (artículo 6 LOPD).

Por lo que se refiere a los datos sobre la salud, para analizar la necesidad de recabar el consentimiento del paciente deben distinguirse dos supuestos: la obtención y tratamiento de los datos sobre la salud y la cesión o comunicación de datos sobre la salud a terceros.

3.4.3.1 **Obtención y tratamiento de los datos sobre la salud**

Con relación a estos datos, la ley exige que el afectado consienta expresamente el hecho de que los mismos puedan ser recabados, tratados y cedidos, salvo que, por razones de interés general, lo disponga una ley (artículo 7.3 LOPD). Pero además, la norma contempla otras dos excepciones a la exigencia del consentimiento en el caso de los datos sanitarios, que son las siguientes: la primera permite el tratamiento de los citados datos cuando el mismo resulte necesario para la prevención o diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto (artículo 7.6 LOPD).

La Agencia de Protección de Datos de la Comunidad de Madrid (APDCM) (2004:31) establece que esto estaría justificado en la vertiente objetiva del derecho a la vida, que anima toda la gestión asistencial y que prevalecería sobre el derecho a la intimidad y a la protección de datos personales. De hecho como ha señalado la jurisprudencia del Tribunal Constitucional, el derecho a la vida prima sobre la libertad ideológica y religiosa (artículo 16, Constitución española) y sobre la libertad personal (artículo 17, Constitución española), ya que sin vida no hay libertad ideológica, sin vida no hay libertad religiosa, y por tanto, sin vida no hay derecho a la intimidad.

Ha de tenerse en cuenta, sin embargo, que la Ley 41/2002 autoriza el acceso a la historia clínica a determinado personal sanitario por razones distintas del diagnóstico o del tratamiento, e incluso al personal administrativo de gestión en razón a sus específicas funciones.

La segunda excepción deriva de la necesidad de habilitar a las Administraciones públicas en el correcto ejercicio de sus funciones y competencias, pero también a los centros sanitarios privados, pues la citada excepción del consentimiento afecta tanto a las instituciones y

centros sanitarios públicos como a los privados y a los profesionales correspondientes, que podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratadas en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad (artículo 8, LOPD). En aplicación de este precepto, debe considerarse suficiente el consentimiento tácito que se deduce de la asistencia voluntaria del interesado al centro o ante el profesional sanitario, con intención de que le resuelva el problema de salud que pudiera existir, no siendo necesario obtener el consentimiento del mismo con la categoría de expreso (APDCM, 2008).

La Recomendación R(97)5, en su defensa de la intimidad en todo lo relacionado a la enfermedad, aconseja que el consentimiento para el tratamiento automatizado de datos relativos a la salud sea libre, expreso y fundamentado con una correcta información, y no hace referencia a que una norma legal pueda eximir del consentimiento patente y específico. En la Recomendación R (97)5 no se prevén excepciones al consentimiento (Sánchez Carazo, 2000).

El Convenio de Oviedo no trata directamente el derecho a dar el consentimiento sobre el tratamiento de los datos de carácter personal relativos a la salud, pero sí defiende el consentimiento ante cualquier intervención sanitaria y, el tratamiento de los datos sanitarios es parte fundamental en la intervención entendida como proceso, creemos que de esta forma, el derecho a consentir o no sobre el manejo y tratamiento de los datos queda defendido en el Convenio de Oviedo (Sánchez Carazo, 2000).

La Ley 41/2002 contiene una regulación distinta en materia de consentimiento. Dentro de los principios básicos, señala que toda actuación en el ámbito sanitario requiere, con carácter general, el previo consentimiento de los pacientes o usuarios. El consentimiento del paciente es la regla general que rige la asistencia sanitaria y éste debe obtenerse después de que el paciente reciba una información adecuada (artículo 2.2). En la misma dirección está el artículo 8 de la Ley 41/2002, que señala que «toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado». No obstante, la extensión de esta regla general del consentimiento prevista para la asistencia sanitaria hacia el tratamiento de los datos sanitarios es incompatible con la excepción de este consenti-

miento establecido en la LOPD, que es a los efectos de los tratamientos de datos personales, la legislación específica. De hecho, la Ley 41/2002 prevé el consentimiento informado para el tratamiento médico, sin hacer mención a la existencia de un tratamiento de datos de carácter personal para el que no se requiere este consentimiento (APDCM, 2004).

Ha de tenerse en cuenta, sin embargo, que aunque no sea preciso recabar el consentimiento del afectado para el tratamiento de sus datos, subsiste incólume la obligación de información. Con todo lo dicho, se puede decir que el consentimiento es un derecho relacionado con el de información; pero deben distinguirse, pues puede haber casos en los que se deba dar información pero no se requiera el consentimiento, como se ha explicado anteriormente. Derechos, pues, autónomos pero muy emparentados, que deben estar en la base de todo tratamiento de datos relativos a la persona.

3.4.3.2 La cesión o comunicación de datos sobre la salud a terceros

Para la cesión de datos la LOPD contempla dos requisitos: el primero, que la cesión lo sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario; y segundo, que se obtenga el previo consentimiento del interesado (artículo 11.1, LOPD).

El primero de los requisitos no admite excepciones, pero el segundo sí, y entre las mismas se encuentra expresamente contemplado el caso de los datos relativos a la salud, respecto de los que la ley indica que no será preciso el consentimiento para la cesión de los mismos a terceros cuando dicha cesión sea necesaria para solucionar una urgencia médica o para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica (artículo 11.2, LOPD). Por otro lado, establece que no se considerará comunicación de datos el acceso de un tercero (encargado del tratamiento) a los mismos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento (artículo 12.1, LOPD).

Como indica Andérez González (2001) la afirmación contenida en este precepto constituye en realidad una habilitación para la posible

contratación externa del tratamiento de datos de carácter personal, sin necesidad de consentimiento del afectado.

Señala Rubí Navarrete (2004) que es cada vez más frecuente la intervención de empresas especializadas en el tratamiento documental, son las que en definitiva vienen a prestar este servicio a las instituciones sanitarias, es decir, son servicios que se externalizan a terceros. La LOPD, a estos efectos distingue entre dos figuras: una la que llama el responsable del fichero o del tratamiento, que es el que decide sobre el destino, el uso, la finalidad de los datos; y otra denominada encargado del tratamiento, que es aquel que presta un servicio al responsable y que supone o implica el acceso a información de terceras personas.

Aunque desde el punto de vista material exista un acceso a la información de terceros, establece una ficción jurídica, de forma que con determinadas garantías, cuando se produce este acceso por parte del que presta el servicio, no hay una cesión de datos, ni comunicación de datos, hay una cobertura jurídica para ese acceso. No obstante, la LOPD establece un sistema de garantías para tratar de conseguir que el acceso a la información, cuando se presta un servicio, tenga el mismo sistema de protección como si el tratamiento de la información lo estuviera realizando el propio responsable.

En primer lugar, el objeto de la prestación es básico, porque conecta directamente con el principio de finalidad en materia de protección de datos, y sólo podrán realizarse aquellos tratamientos que respondan a una finalidad adecuada para el objeto de prestación. Tiene que incorporarse, además, la advertencia expresa al que presta el servicio de que sólo podrá tratar los datos para esa finalidad y no para finalidades distintas; tiene que advertirse, también, que el que presta el servicio no podrá ceder los datos a terceros; y que cuando termine la prestación del servicio, que puede en principio ser indefinida, deberá destruir la información o devolverla al responsable del fichero (artículo 12 LOPD).

Tiene que incorporarse la exigencia, de que el que presta el servicio debe cumplir las mismas medidas de seguridad que fueran exigibles al responsable del fichero, es decir, en el caso de los datos de salud, las medidas de seguridad de nivel alto, establecidas en el Reglamento de desarrollo de la LOPD (Real Decreto 1790/2007). La importancia del cumplimiento de todos los requisitos referidos es grande toda vez que, en ausencia de los mismos, se estará ante un

caso de cesión de datos que en principio requiere del consentimiento del afectado.

La LOPD define, en el artículo 3.f) como disociación, «todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable». La disociación en el ámbito de la investigación epidemiológica, de salud pública, de investigación o docencia excluiría la vigencia de la legislación de protección de datos personales, al no tener como objeto información sobre personas físicas identificadas o identificables. No obstante, la Ley 41/2002 establece esta disociación como regla general, lo que no impide su custodia disociada por la posibilidad de su asociación, de modo que esta disociación se convierte en una medida de seguridad. En cualquier caso, el acceso a la historia clínica con fines epidemiológicos, de salud pública, de investigación o de docencia no debe ser indiscriminado sino que también queda limitado estrictamente a los fines específicos de cada caso.

Existen otros supuestos que justifican un acceso, o una cesión de la historia clínica a terceras personas, esto hace referencia, por ejemplo, a la comunicación de datos de la historia clínica a los órganos judiciales. La propia LOPD establece que, si bien la comunicación de datos a un tercero exige el previo consentimiento del interesado, es posible esta cesión sin consentimiento, entre otros supuestos, cuando ésta se encuentre autorizada en una ley o cuando ésta comunicación tenga por objeto los órganos judiciales o el Ministerio Fiscal; esto es corroborado por la Ley 41/2002.

El acceso a la historia clínica por parte de los órganos judiciales y por tanto la cesión de información clínica a los tribunales está vinculado a otro derecho, el de tutela judicial (artículo 24.1 de la Constitución española) que es también un derecho fundamental y que esta al mismo nivel que el derecho a la intimidad. De hecho, el propio conocimiento de los Tribunales es garantía de todos los derechos e intereses legítimos. Eso no obsta para que el acceso a los datos y documentos de la historia clínica quede limitado estrictamente a los fines específicos de cada caso. Es así que la APDCM (2004:45) señala que los jueces deben limitar su petición de acceso a la historia clínica a los datos imprescindibles y los médicos vista a veces la ambigüedad de algunas peticiones judiciales, tienen que aplicar el principio de proporcionalidad, dando la información que consideren necesaria en cada caso, y pidiendo aclaraciones, si resulta necesario a los propios órganos judiciales.

Existen otras posibles comunicaciones de datos de historias clínicas no previstas en la Ley 41/2002 y que se plantean frecuentemente. Es posible la comunicación de datos de la historia clínica que tengan relevancia económica a la Intervención y a las unidades de control financiero, aunque éstas no tengan carácter de personal sanitario. El artículo 11.2 a) de la LOPD permite la comunicación de datos sin consentimiento del interesado cuando exista previsión legal. Pues bien, tanto la legislación estatal como la autonómica establece que todos los actos, documentos y expedientes de la Administración de los que se deriven derechos y obligaciones de contenido económico, serán objeto de control por parte de la Intervención de la Administración; lógicamente la Intervención sólo puede acceder a datos que tengan repercusiones económicas como instrumento para controlar la legalidad del gasto (APDCM, 2008).

En relación con el tratamiento de datos de salud con fines policiales, hay que señalar que el artículo 22.3 de la LOPD permite la recogida y tratamiento de los datos de salud y del resto de datos especialmente protegidos; que podrá realizarse «exclusivamente en los supuestos que sean absolutamente necesarios para los fines de una investigación concreta, sin perjuicio del control de la legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales». La APDCM (2004:49) señala que la policía deberá solicitar la autorización judicial como regla general, la misma que se suele dar con rapidez, y que es un instrumento adecuado para salvaguardar las exigencias del artículo 22.3 de la LOPD referidas al control de legalidad de la actuación administrativa.

Por último, las cesiones destinadas a centros sanitarios de distintos países es cada vez más frecuente en el ámbito de la Unión Europea dentro del principio de libre circulación de pacientes, pero cada vez más se extiende a otros países fuera del ámbito de la Directiva 95/46/CE, por lo que en este caso hay que estar a la normativa relativa a transferencias internacionales de datos, que prohíbe las transferencias con destino a países que no tengan un nivel de protección equiparable sin consentimiento del interesado, en el marco del acuerdo de Puerto Seguro o con autorización del Director de la Agencia Española de Protección de Datos después de haber comprobado que existen garantías adecuadas.

3.4.4 PRINCIPIO DE DATOS ESPECIALMENTE PROTEGIDOS

La ley incluye dentro de esta categoría a los datos relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual (artículo 7 LOPD).

Respecto de los datos sanitarios este régimen de especial protección se concreta, básicamente, en que los mismos sólo podrán ser recabados, tratados y cedidos en los términos que se han dejado referidos anteriormente, y también en el hecho de que los citados datos son merecedores de la adopción de medidas técnicas de seguridad de nivel alto, establecidas en el Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007).

3.4.5 PRINCIPIO DE SEGURIDAD DE LOS DATOS

El Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías[15] ha afirmado que la seguridad informática es un imperativo ético para garantizar el respeto a los derechos humanos y libertades del individuo y la confidencialidad de sus datos. La seguridad informática es la garantía de que sólo acceden a la información las personas autorizadas y de que no se producen esos accesos por parte de terceras personas no autorizadas. Esta es la razón por la que los ficheros que contengan datos considerados especialmente protegidos, como los datos de salud, estén sometidos a las citadas medidas de seguridad de nivel alto, que tuvo un plazo de implantación después de sucesivas prórrogas hasta el 26 de junio de 2002.

Las medidas de seguridad de los ficheros informatizados y no informatizados (manuales) están reguladas en el Reglamento de Desarrollo de la LOPD aprobado por Real Decreto 1720/2007, de 21 de diciembre, que distingue entre medidas de seguridad de nivel básico, medio y alto.

Las medidas de seguridad incluidas en cada uno de los niveles tienen la condición de mínimos descritos exigibles, sin perjuicio de las

---

[15] En el documento «Principios Éticos de la Sanidad en la Sociedad de la Información», elaborado el 30 de julio de 1999, por el Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías.

disposiciones legales o reglamentarias específicas que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

De conformidad con el Reglamento de desarrollo de la LOPD los datos de salud exigen la aplicación del nivel alto en lo referente a aspectos técnicos y organizativos que garanticen la confidencialidad e integridad de los datos, evitando, en consecuencia su alteración, pérdida o acceso no autorizado.

Es una infracción grave mantener ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaría se determinan (APDCM, 2004).

En este sentido, el Real Decreto 1720/2007, de 21 de diciembre, establece las medidas de seguridad de los ficheros informatizados en los siguientes artículos:

— Artículos 89 a 94, regulan las de nivel básico (Documento de Seguridad; funciones y obligaciones del personal; registro de incidencias; control de acceso; gestión de soportes y documentos; identificación y autentificación; copias de respaldo y recuperación).

— Artículos 95 a 100, las de nivel medio (Responsable de Seguridad; auditoría; gestión de soportes y documentos; identificación y autentificación; control de acceso físico; registro de incidencias).

— Artículos 101 a 104, las de nivel alto (gestión y distribución de soportes, copias de respaldo y recuperación; registro de accesos; telecomunicaciones).

Por otra parte, una de las principales novedades del Real Decreto 1720/2007, de 21 de diciembre, es que, por primera vez se regulan las medidas de seguridad para los ficheros no automatizados (manuales). En este sentido, se han seguido algunas de las medidas de seguridad contenidas en la Recomendación 2/2004, de 30 de julio, sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas y Recomendación 1/2005, de 5 de agosto, sobre Archivo, Uso y Custodia de la Documentación que compone la Historia Social no informatizada por parte de los Centros Públicos de Servicios Sociales de la Comunidad de Madrid ambas de la

Agencia de Protección de Datos de la Comunidad de Madrid (APDCM, 2008).

Otra novedad introducida por el Real Decreto 1790/2007, de 21 de diciembre, es la previsión de que las medidas de seguridad «genéricas» de los ficheros automatizados resultan de aplicación a los ficheros no automatizados. Estas medidas son, entre otras, la elaboración del documento de seguridad –que suele ser un documento en formato papel, o en su caso, un documento en Word o PDF–; las obligaciones respecto al encargado del tratamiento, cuyo acceso deberá estar delimitado en el documento de seguridad; y el régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento –debiendo ser autorizado este supuesto por el responsable o encargado– constando dicha autorización en el documento de seguridad.

Sin perjuicio de la adopción de estas medidas de seguridad del Real Decreto 1720/2007, de 21 de diciembre, contiene, además, tres criterios específicos para los ficheros no automatizados: 1) los criterios referentes al archivo, con una referencia a la legislación aplicable en esta materia que será la relativa a la normativa que regula los Archivos; 2) los referentes a los dispositivos de almacenamiento, que deberán disponer de mecanismos que obstaculicen su apertura; y 3) los referentes a la custodia de soportes, en virtud de los cuales la persona encargada de la custodia, mientras la documentación en formato papel esté en proceso de revisión o tramitación, deberá vigilarla e impedir que cualquier persona no autorizada pueda acceder a ella.

Por último, en el supuesto de los ficheros parcialmente automatizados («mixtos»), la parte del fichero que sea automatizada deberá adoptar las medidas de seguridad de acuerdo con lo establecido para dichos ficheros automatizados, mientras que la parte de ese mismo fichero que no sea automatizada, adoptará las referentes a los ficheros no informatizados; si bien, a efectos de la creación del fichero, en la disposición general de creación y en su inscripción en el Registro se realizarán las más altas medidas de seguridad de las que puedan corresponderles (APDCM, 2008).

En este sentido, en el de aplicación a los ficheros sanitarios de la totalidad de las medidas contenidas en el reglamento, han de interpretarse los preceptos correspondientes de la Ley 41/2002, que deben ser integrados correctamente dentro del marco del ordenamiento jurí-

dico y en consecuencia de la legislación vigente en materia de protección de datos personales.

3.4.6 PRINCIPIO DE DEBER DE SECRETO

Otro principio fundamental es el deber de secreto. El artículo 10 de la LOPD señala que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsisten aún después de finalizar sus relaciones con el titular del fichero, o en su caso con el responsable del mismo.

No debe confundirse el deber de secreto con el secreto profesional al que están sometidas determinadas personas en función de la profesión que ejercen. Este deber de secreto es un deber genérico que alcanza a cualquier persona que intervenga en el tratamiento de los datos.

La Agencia Española de Protección de Datos recomienda la inclusión de cláusulas específicas en esta materia en los contratos laborales que suscriban las Administraciones Públicas de su ámbito de actuación con empleados públicos. Igualmente, el trabajador estará obligado a atender las instrucciones relativas a la seguridad de los datos de carácter personal contenidas en las políticas de seguridad y en el documento de seguridad y difundidas, en su caso, por el responsable del fichero o el responsable de seguridad, de conformidad con lo establecido en el Reglamento de desarrollo de la LOPD (APDCM, 2008).

Lógicamente, estas obligaciones no son meramente teóricas sino que su omisión es una infracción grave. Así, el artículo 44.3 de la LOPD señala que es una infracción muy grave «la vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7».

Esta obligación de secreto queda reforzada por la Ley 41/2002, en ella se establece que la persona que elabore o tenga acceso a la información y documentación clínica está obligada a guardar la debida reserva (artículo 2.7). Lo mismo se vuelve a repetir en el artículo 16.6 cuando señala que el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

3.4.7 PRINCIPIO DE COMUNICACIÓN DE DATOS

Este principio hace referencia al cumplimiento de determinadas obligaciones en el caso de que se produzca una cesión de datos personales, es decir, una revelación de éstos a persona distinta del interesado. En todo caso, para que pueda llevarse a cabo una cesión legal de datos, deberán coincidir varios elementos fundamentales:

— Una premisa, que la cesión se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.

— Una condición general, que exista previo consentimiento del interesado.

— Una información necesaria, que el interesado o afectado tenga conocimiento de la identidad del cesionario y de la finalidad para la que se van a ceder los datos (APDCM, 2004).

Hay que tener en cuenta una vez más que según el artículo 44.4.b) de la LOPD cuando se realice una comunicación o cesión de los datos de carácter personal fuera de los casos en que estén permitidas se considerará como una infracción muy grave. La problemática con la cesión de datos ha sido vista en extenso en el principio de consentimiento del interesado.

El que no sea necesario pedir consentimiento del interesado en un momento dado para realizar una cesión, no significa que se le deje de informar. Así la LOPD señala que el responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando asimismo la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario (artículo 27, LOPD).

Cuando la cesión de datos relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero, o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. Nuevamente se reitera el criterio de que en caso de colisión de los derechos a la vida o integridad física y el derecho a la protección de datos, debe prevalecer el primero.

En el supuesto de que la finalidad sea la realización de estudios epidemiológicos, con el objeto de velar por la salud desde un punto

de vista preventivo, la cesión de datos para estos fines podrá efectuarse sin consentimiento del interesado, siempre que el estudio epidemiológico se realice en los términos que establezca la legislación específica sobre sanidad (APDCM, 2008).

Por ejemplo, existen cesiones de datos sanitarios de la Administración Pública a empresas privadas que se encuentran reguladas y que son necesarias para una buena atención médica. Sánchez Carazo (2000:168) pone como ejemplo el caso de un paciente al que se le coloca una prótesis, es necesario que el fabricante conozca a las personas que se les ha puesto su producto por si hubiese algún defecto en el lote o cualquier otra anormalidad, por lo que se deberá comunicar al interesado la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

En los últimos años la protección de los datos sanitarios de los pacientes se ha visto reducida, entre otras causas, porque los hospitales públicos, concertados y privados tienen que llevar una contabilidad rigurosa ante la gran importancia que tiene el gasto sanitario. Para ello se van a rendir cuentas e informar tanto de los pacientes como de sus tratamientos. Por tanto, el diagnóstico de entrada en el centro, los procedimientos realizados y el diagnóstico de salida han de comunicarse a las entidades pagadoras: compañías de seguros, al Servicio de Salud a cargo de la Comunidad Autónoma o entidades colaboradoras. Estas obligaciones de comunicar información representan un cercenamiento considerable de la intimidad y, por ello, ponen en peligro la protección de datos de carácter sanitario. Sin embargo, resultan necesarias para controlar costes, por lo que, al menos, el paciente deberá estar informado de los datos que se ceden a las entidades que van a pagar el proceso asistencial, incluso los propios médicos tendrán que facilitar datos sanitarios para justificar los reembolsos (Sánchez Carazo, 2000).

Joachim Jacob (1999:312) citado por Sánchez Carazo (2000:169) explica que se ha acordado que los seguros de enfermedad no deberían reunir todo un conjunto de datos sanitarios relativos a las personas aseguradas, pues no se puede convertir a los asegurados en personas transparentes como el cristal y, para la conservación y utilización de tales datos, existen limitaciones jurídicas que contribuyen a proteger la intimidad del paciente. Sin embargo, se debe tener conciencia del hecho que, hoy más que nunca, es más necesario y a la vez más

difícil, proteger los datos de carácter médico frente a los intereses económicos.

Finalmente, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, exige que los datos de identificación personal del paciente se separen de los de carácter clínico asistencial, de forma que, como regla general, quede asegurado el anonimato del paciente, salvo que haya dado su consentimiento para no separarlos.

3.4.8 PRINCIPIO DE ACCESO A DATOS POR CUENTA DE TERCEROS

El acceso a datos por cuenta de terceros es el acceso permitido a terceros que no tienen la condición de responsable de fichero, usuario o interesado, sin que por ello se produzca una cesión o comunicación de datos. Se trata de la posibilidad de que los datos personales puedan ser tratados por personas distintas de los usuarios de la propia organización del responsable del fichero, por encargo de éste.

Esta tercera persona se convierte, en este caso, en *encargado de tratamiento*, y presta servicios al responsable del fichero, siempre que dichos servicios tengan como objeto una finalidad lícita y legítima[16]. En estos casos, la LOPD regula la relación entre el responsable del fichero y el encargado del tratamiento, estableciendo una serie de obligaciones encaminadas a garantizar la seguridad del tratamiento de los datos personales (APDCM, 2004).

La relación que se establece para el tratamiento de los datos personales debe regularse en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, en el que conste:

— Que el encargado únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.

---

[16] Por ejemplo: la contratación por parte del hospital del depósito, custodia y gestión integral del archivo de la documentación clínica. El soporte y mantenimiento de un servidor que realiza una empresa para un organismo público.

— Las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

— Que el encargado del tratamiento no cederá los datos a otras personas, ni siquiera para su conservación.

— Que una vez cumplida la prestación, los datos serán destruidos o devueltos al responsable, al igual que cualquier soporte o documentos en que consten datos objeto de tratamiento.

El encargado del tratamiento responderá de las infracciones en las que hubiera incurrido personalmente, equiparándose en tal caso su figura, en materia de responsabilidad, a la del responsable del tratamiento, con independencia de las posibles y concretas responsabilidades propias del responsable de tratamiento. No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquel al que hubiera encomendado la prestación de un servicio.

Respecto a la figura del encargado del tratamiento, el Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007, de 21 de diciembre) regula la posibilidad de que dicho encargado del tratamiento subcontrate a su vez el servicio que ha contratado con el responsable del fichero. Para que esta subcontratación tenga lugar será necesario que el encargado del tratamiento haya obtenido la autorización del responsable del fichero. Esta subcontratación se efectuará siempre en nombre y por cuenta del responsable del fichero.

Sin embargo, será posible la subcontratación sin necesidad de autorización del responsable del fichero siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y la empresa con la que se vaya a subcontratar.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos para el contrato entre el responsable del fichero y el encargado del tratamiento.

En este caso, el subcontratista será considerado encargado del tratamiento. En el supuesto que durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del fichero los extremos señalados anteriormente.

Por último, el Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007) contempla la posibilidad de que los derechos de acceso, cancelación, oposición y rectificación, se ejerciten ante un encargado del tratamiento. En este caso, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición (APDCM, 2008).

3.4.8.1 **Proveedor de servicios de *cloud computing* y tratamiento de datos personales**

El modelo de *cloud computing* hace posible que tanto los proveedores de servicios como los datos almacenados en la *nube* se encuentren ubicados en cualquier punto del planeta.

«*Cloud computing* es un modelo que permite el acceso bajo demanda y a través de la red, a un conjunto de recursos compartidos y configurables (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con esfuerzo mínimo de gestión e interacción con el proveedor del servicio» (NIST, 2011:6).

El *National Institute of Standars and Technology* (NIST) es un organismo internacional de los Estados Unidos que se dedica a definir estándares y tecnología, el cual tiene un laboratorio dedicado específicamente a *cloud computing* que se encarga de hacer definiciones y especificaciones de los modelos de la nube. Las categorías definidas por el NIST y aceptadas universalmente son modelos de despliegue (nubes públicas, privadas, híbridas y comunitarias) y modelos de servicio (software como servicio «SaaS», plataforma como servicio «PaaS» e infraestructura como servicio «IaaS»).

Las aplicaciones de *cloud* en el sector público y privado comprenden la posibilidad de trastear de la tierra a la nube los datos personales de empleados, clientes y ciudadanos en general. Estos pueden ser almacenados, procesados y administrados por empresas que proveen servicios de *cloud* denominados *cloud service provider* (CSP). Como es sabido, la información no está en la nube, sino distribuida en poderosos data centers ubicados en varias partes del mundo (Remolina Angarita, 2013).

El cliente que contrata servicios de *cloud computing* sigue siendo responsable del tratamiento de los datos personales. Aunque los contrate con una gran compañía multinacional la responsabilidad no se desplaza al prestador del servicio, ni siquiera incorporando una cláusula en el contrato con esta finalidad.

Con esta información debe decidir para qué datos personales contratará servicios de *cloud computing* y cuáles prefiere mantener en sus propios sistemas de información. Esta decisión es importante porque delimitará las finalidades para las que el proveedor de *cloud* puede tratar los datos. En consecuencia, debe garantizarse expresamente que no utilizará los datos para otra finalidad que no tenga relación con los servicios contratados.

El que ofrece la contratación de *cloud computing* es un prestador de servicios que en la ley de protección de datos de España tiene la calificación de «encargado del tratamiento».

Pero, en todo caso:

— El cliente que contrata servicios de *cloud computing* sigue siendo responsable del tratamiento de los datos por lo que la normativa aplicable al cliente y al prestador del servicio es la legislación española sobre protección de datos (Ley Orgánica 15/1999, de fecha 13 de diciembre, y Reglamento de Desarrollo – RLOPD aprobado por Real Decreto 1720/2007).

— La aplicación de la legislación española no puede modificarse contractualmente.

— Aunque le informen de que los datos personales están disociados, no cambia la ley aplicable ni la responsabilidad del cliente y del prestador del servicio.

El cliente debe solicitar y obtener información sobre si intervienen o no terceras empresas (subcontratistas) en la prestación de servicios de *cloud computing*.

Lo habitual es que intervengan terceras empresas. De ser así el cliente:

— Tiene que dar su conformidad a la participación de terceras empresas, al menos delimitando genéricamente los servicios en los que participarán (p. ej. en el alojamiento de datos). Para ello, el prestador del servicio de *cloud computing* tiene que informarle sobre la tipología de servicios que pueden subcontratarse con terceros.

— Tiene que poder conocer las terceras empresas que intervienen (p. ej. pudiendo acceder a una página web o a través de otras opciones que le facilite el prestador del servicio).

— El proveedor de *cloud* debe asumir en el contrato que los subcontratistas le ofrecen garantías jurídicas para el tratamiento de los datos equivalentes a los que él mismo asume.

— El contrato que firma ha de incorporar cláusulas contractuales para la protección de los datos personales.

La localización de los datos tiene importancia porque las garantías exigibles para su protección son distintas según los países en que se encuentren. Los países del Espacio Económico Europeo (EEE) ofrecen garantías suficientes y no se considera legalmente que exista una transferencia internacional de datos. El Espacio Económico Europeo está constituido por los países de la Unión Europea e Islandia, Liechtenstein y Noruega.

Si los datos están localizados en países que no pertenecen al Espacio Económico Europeo habría una transferencia internacional de datos, en cuyo caso, y dependiendo del país en que se encuentren, deberán proporcionarse garantías jurídicas adecuadas.

Se considera una garantía adecuada que el país de destino ofrezca un nivel de protección equivalente al del Espacio Económico Europeo y así se haya acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea[17]. En ese caso será sufi-

---

[17] Países con un nivel adecuado de protección: 1) Suiza, Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000; 2) Canadá, Decisión 2002/2/CE de la Comisión de fecha 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos; 3) Argentina, Decisión 2003/490/CE de la Comisión de fecha 30 de junio

ciente con hacer constar la transferencia en la notificación del fichero realizada a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos.

Las proporcionadas por las empresas ubicadas en los Estados Unidos que hayan suscrito los principios de Puerto Seguro[18]. Al igual que en el caso anterior será suficiente con hacer constar la transferencia en la notificación del fichero a la Agencia Española de Protección de Datos.

---

de 2003; 4) Guernsey, Decisión 2003/821/CE de la Comisión de fecha 21 de noviembre de 2003; 5) Isla de Man, Decisión 2004/411/CE de la Comisión de fecha 28 de abril de 2004; 6) Jersey, Decisión 2008/393/CE de la Comisión de fecha 8 de mayo 2008; 7) Islas Feroe, Decisión 2010/146/UE de la Comisión de fecha 5 de marzo de 2010; 8) Andorra, Decisión 2010/625/UE de la Comisión de fecha 19 de octubre de 2010; 9) Israel, Decisión 2011/61/UE de la Comisión de fecha 31 de enero de 2011; 10) Uruguay, Decisión 2012/484/UE de la Comisión de fecha 21 de agosto de 2012; y 11) Nueva Zelanda; Decisión 2013/65/UE de la Comisión de fecha 19 de diciembre de 2012. Agencia Española de Protección de Datos (2015): *«Transferencia internacionales de datos»* [en línea]: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php#paises [Consulta: 18/06/2015]

18 *«El Tribunal de Justicia de la Unión Europea (TJUE) ha hecho pública hoy la sentencia que anula la Decisión de la Comisión 2000/520/CE que establece el nivel adecuado de protección de las garantías para las transferencias internacionales de datos a EEUU ofrecidas por el acuerdo de Puerto Seguro publicado por su Departamento de Estado. El Tribunal afirma que el objetivo de la Directiva 95/46/CE de Protección de Datos no es tanto asegurar la libre circulación de la información sino, sobre todo, garantizar el elevado nivel de protección de los derechos fundamentales consagrados por los artículos 7 y 8 de la Carta de Derechos Fundamentales de la UE. La sentencia proclama que la Decisión de Puerto Seguro es inválida por dos motivos: 1) Porque entiende que prevalece incondicionalmente y sin ninguna limitación «la seguridad nacional, el interés público o el cumplimiento de la ley» sobre los derechos fundamentales a la intimidad y la protección de datos, sin otorgar a los ciudadanos europeos ningún medio para obtener la tutela efectiva de esos derechos. 2) Porque no otorga a los Estados miembros un margen suficiente para suspender las transferencias en caso de que estos apreciaran una vulneración de los derechos de los ciudadanos europeos».* Agencia Española de Protección de Datos (2015): *«El TJUE declara inválida la Decisión de la Comisión que declara el nivel adecuado de protección de Puerto Seguro»* [en línea]: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_06-ides-idphp.php[Consulta: 18/10/2015]

En otro caso, la transferencia internacional de datos necesitará autorización del Director de la Agencia Española de Protección de Datos, que podrá otorgarse en caso de que el exportador de datos aporte garantías adecuadas (AEPD, 2013).

La computación en la nube ofrece gran número de beneficios y ventajas para los usuarios finales, organizaciones y empresas, así como a la industria y en general a la sociedad. También tiene inconvenientes que es necesario tener presente para su adopción y posterior migración a la nube, especialmente en temas de seguridad y privacidad de los datos (Joyanes Aguilar, 2012).

3.4.9 PRINCIPIO DE FINALIDAD LEGÍTIMA

De acuerdo con lo establecido en la LOPD, los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles[19] con aquellas para las que los datos hubieran sido recogidos (artículo 4.1 y 4.2 LOPD).

Desde el punto de vista positivo, parece evidente que deberán ser tratados todos aquellos datos e informaciones sanitarias que se consideren trascendentales para el conocimiento veraz y actualizado del estado de salud del paciente, incorporándose a la historia clínica, ya que la misma tiene como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que bajo criterio médico permitan conformar dicho conocimiento (Sánchez-Caro y Abellán, 2004).

En cambio, desde el punto de vista negativo, no se considera incompatible el tratamiento de los datos de carácter personal que se refieran a la salud, cuando dicho tratamiento resulte necesario para la prevención o diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sani-

---

[19] Los datos del Padrón Municipal de Habitantes pueden usarse para enviar información a los vecinos sobre la apertura de un nuevo Centro de Servicios Sociales (finalidad compatible). Sin embargo, no pueden utilizarse para enviar una felicitación de navidad o para pedir el voto (finalidad incompatible).

tario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

3.5 DERECHOS BÁSICOS DE LOS CIUDADANOS EN MATERIA DE PROTECCIÓN DE DATOS SOBRE SALUD

A objeto de que los ciudadanos puedan conocer en todo momento la información que sobre los mismos se haya podido recabar, e incluso conseguir que se rectifique o cancele en su caso, la LOPD configura una serie de derechos independientes entre sí.

3.5.1 EL DERECHO DE ACCESO A LA INFORMACIÓN CLÍNICA POR LOS PACIENTES

Hasta hace pocos años el acceso a la historia clínica y a los datos sanitarios en esa relación de beneficencia-paternalismo que el médico tenía con sus pacientes, era poco común o mejor dicho extraordinaria. Durante muchos años la información se consideraba un privilegio que el médico podía o no conceder a sus pacientes pero siempre según su criterio, pero la medicina ya no puede ser un arte silencioso. El médico ha de ser consciente que informar es una exigencia del deber de beneficencia que tiene hacia sus pacientes (Sánchez Carazo, 2000).

Aunque dar la información al paciente se trate de un elemental problema de derecho individual, es difícil cambiar las formas tradicionales de comportamiento en que el médico callaba lo que creía conveniente, y por supuesto, el paciente no podía acceder a sus datos sanitarios. Pero el informar, el dar acceso a los datos sanitarios, no es un acto más, es más bien un proceso dentro del acto médico. Así, aunque algunos piensen que puede ser una pérdida de tiempo, o que el paciente no comprenderá correctamente, o bien, que el conocimiento de la verdad puede crear estados de ansiedad y angustia, la realidad es bien distinta. Sí, es cierto que puede haber pacientes que no quieran saber, y este derecho hay que respetarlo, en la mayoría de los casos la información, el conocimiento del proceso, mejora la relación médico-paciente, y con ella, su acción terapéutica (Blas Orbán, 2006).

El derecho de acceso que de acuerdo a la LOPD consiste en el derecho del interesado a solicitar y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, así como sobre el origen de dichos datos, y de las comunicaciones realizadas o que se prevean hacer de los mismos (artículo 15.1 LOPD).

En el ámbito sanitario, cuando se habla del derecho de acceso a los datos personales, se refiere a un tipo de información peculiar como es la información clínica, donde la regla general es que la asistencia sanitaria prestada a un ciudadano es la única razón que justifica el acceso a la misma, cualquier otra razón de acceso a la información debe responder a un interés legítimo susceptible de protección y estar convenientemente motivada (Sánchez-Caro y Abellán, 2004).

Este derecho de acceso a la historia clínica está justificado tanto desde el respeto al derecho fundamental a la protección de datos personales y la libertad informática, que implica el acceso a la propia información personal, como desde el propio respeto del derecho a la salud y a la vida, que justifica el conocimiento de todos aquellos datos e informaciones relevantes sobre el propio estado de salud. Su incumplimiento, señala la APDCM (2004:40) «es una lesión grave del derecho fundamental a la intimidad, a la protección de datos y justifica no sólo una acción de tutela ante las Agencias de Protección de Datos Personales, sino la apertura de un procedimiento contencioso administrativo o un procedimiento civil preferente y sumario de tutela de los derechos fundamentales».

La LOPD y sus normas de desarrollo, cuando se ejerce el derecho de acceso, atribuyen más garantías al titular de los datos que al responsable del tratamiento de esos datos, y por eso la norma establece que el que ejerce el derecho es el que puede optar por cuál es el procedimiento para el acceso a la información: visualizarlo por la pantalla, exigir una copia, u otros supuestos que están en ese reglamento. La regla general es que la forma de acceder a la información depende más o es más un derecho del afectado que un derecho del responsable, y por tanto, el responsable no puede imponer al afectado una determinada modalidad, salvo que desde el punto de vista técnico la única solución técnica posible sea la que ofrezca la institución sanitaria (Rubí Navarrete, 2004).

La regulación del acceso a la historia clínica está contenida en la Ley 41/2002 Básica de Autonomía del Paciente, de acuerdo con dicha

norma podemos distinguir diversos tipos de acceso a la información de la historia clínica: por el paciente, por la inspección, para fines estadísticos, para fines científicos o de investigación, y por otras personas o autoridades.

El acceso del paciente a la información de la historia clínica parece evidente, dado que la misma se redacta y se conserva para facilitar su asistencia, lo que supone dar a conocer al paciente la biografía patológica contenida en su historia clínica. Así lo establece la Ley 41/2002 al reconocer este derecho al paciente, que abarca la posibilidad de obtener copia de los datos consignados (artículo 18.1 Ley 41/2002).

Ahora bien, el acceso del paciente o de su representante puede deberse a un interés particular o a un interés sanitario. En el caso de querer acceder por un interés particular hay que tener en cuenta que se pueden establecer dos excepciones a dicho acceso, los datos incorporados a la historia clínica por terceros en interés terapéutico del paciente y las anotaciones subjetivas que puede hacer el médico en un momento determinado, siempre que tengan trascendencia clínica, en otro caso deberían incluirse en la historia clínica. En el acceso del paciente a su historia clínica por interés sanitario no rigen las anteriores excepciones, ya que la consulta de la historia clínica es de capital importancia para el médico que vaya a valorar de nuevo al paciente; en tales casos, como es obvio, el expediente podría ser remitido directamente al profesional sanitario, si así se considera conveniente (Blas Orbán, 2006).

Como ya se ha dicho, la Ley 41/2002 establece que el derecho de acceso por parte del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella, recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

Puente Escobar (2004:34) señala «que el problema estribará en determinar que habrá de entenderse por anotaciones subjetivas, dado que la reserva del facultativo no debería en modo alguno impedir un adecuado tratamiento asistencial del paciente que pudiera en el futuro acudir a un nuevo facultativo o a un nuevo centro sanitario, en virtud de su derecho de libre elección, consagrado en la Ley 41/2002 ni menoscabar el derecho a conocer, consagrado por las normas inter-

nacionales ratificadas por España». Por ello, cualquier interpretación de la norma exigiría efectuar una interpretación restrictiva de lo que haya de entenderse por anotación subjetiva que no menoscabe los derechos del paciente ni perjudique su futuro tratamiento médico.

En cuanto a los pacientes fallecidos, la Ley 41/2002 dispone que los centros sanitarios y facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a los mismos, por razones familiares o de hecho, salvo que el fallecido hubiese prohibido expresamente y así se acredite. Sin embargo, advierte la norma que no se facilitará información que afecte a la intimidad del fallecido ni a la que se refiera a las anotaciones subjetivas de los profesionales o la que perjudique a terceros (artículo 18.4 Ley 41/2002).

Por último, regula la ley el caso del acceso de un tercero a la historia clínica motivado por un riesgo de salud, estableciendo, en virtud del principio de proporcionalidad, que dicho acceso se limitará a los datos pertinentes.

3.5.2 LOS DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN DE LA INFORMACIÓN SANITARIA

Los derechos de rectificación y cancelación[20] conceden la posibilidad al interesado de exigir al responsable del fichero que cumpla con el principio de calidad de datos y de finalidad, pudiendo instarle a rectificar aquellos cuyo tratamiento no se ajuste a las previsiones de la ley, y en particular cuando los mismos resulten ser inexactos o incompletos; o a cancelarlos cuando hayan dejado de ser necesarios para la finalidad para la cual hubieran sido registrados (artículo 4.5 LOPD). El objetivo último es que los datos se mantengan de forma adecuada, pertinente y no excesiva en relación con el ámbito y las finalidades legítimas para las que se recogieron.

---

[20] Cancelar significa bloquear los datos, manteniéndolos exclusivamente a disposición de las Administraciones Públicas competentes y de los Jueces y Tribunales, y borrándolos cuando hayan prescrito las posibles responsabilidades derivadas del tratamiento (APDCM, 2008).

Los derechos de rectificación y cancelación de datos personales son derechos personalísimos. Como en el caso del derecho de acceso, el representante legal del afectado puede actuar cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos (García – Berrio 2003).

Por lo que se refiere a los datos sanitarios y a la posibilidad de ejercicio de los derechos de rectificación y cancelación de los mismos, su conservación, debe asegurarse, total o parcialmente, al menos durante el tiempo razonablemente necesario para alcanzar el propósito concreto que justificó su recogida y que debe ser cuando menos aquel que bajo un criterio médico se establezca en el centro o área sanitaria para la asistencia del paciente en el curso de la enfermedad que justificó la creación de la documentación clínica (Sánchez-Caro y Abellán, 2004).

Señala la Agencia de Protección de Datos de la Comunidad de Madrid (2004:50) que, «en el ámbito sanitario, la cancelación de los datos es de enorme dificultad ya que está en contradicción con la eficacia de la gestión sanitaria y la necesidad de mantener el contenido completo de la historia clínica, que evite el error en las valoraciones o la repetición de pruebas diagnósticas».

Asimismo, debe significarse que la conservación de la documentación clínica debe garantizar la preservación de la información y no necesariamente el soporte original. No obstante, además del motivo de la atención al paciente, pueden existir otros intereses legítimos de epidemiología, de investigación o de organización y funcionamiento del Sistema Nacional de Salud que justifiquen la conservación de la documentación clínica. En estos casos, siempre que sea compatible con los fines perseguidos, deben tratarse los datos anónimamente al objeto de impedir la identificación directa o indirecta de los sujetos implicados (artículo 17 Ley 41/2002).

Sánchez Carazo (2000:162) considera un caso especial respecto al derecho de cancelación la realización de estudios epidemiológicos, «en estos casos se requiere un largo proceso de mantenimiento de datos personales con vistas al seguimiento de enfermedades y que implican el almacenamiento de datos que reflejan fielmente el estilo de vida del afectado, y en los que informaciones aparentemente irrelevantes pueden adquirir, a la larga, una gran trascendencia». Se plantea por tanto, un conflicto entre el derecho de cancelación de los da-

tos y la necesidad de conservarlos para la realización de estudios epidemiológicos, para los que el mantenimiento de los datos es imprescindible.

Si no se realizara investigación médica, la mortalidad y morbilidad de un buen número de patologías no disminuiría, pero también es cierto que una gran parte de la investigación puede hacerse con datos disociados. Tampoco hay que olvidar que aunque pueda resultar más cómodo almacenar muchos datos por si acaso y trabajar con todos ellos, hay que tener en cuenta que los datos que se han de recoger deben ser pertinentes, como también han de serlo los datos con los que se trabajen. En muchos de ellos no será necesario conservar los datos identificativos, y en estos, es necesario adaptar las medidas necesarias para que la disociación de datos no altere la información sanitaria. En la circunstancia en que los datos sanitarios no se puedan hacer anónimos, será necesario conservar los datos identificativos con las medidas necesarias para proteger el derecho a la intimidad del paciente (Salcedo Beltrán, 2006).

Todo lo expuesto no impide que se lleve a cabo la rectificación correspondiente de los datos erróneos incluidos en la historia clínica cuando se tenga constancia de ellos, pues si bien no se prevé nada expreso en la Ley 41/2002, se establece en ella la obligación de las administraciones sanitarias de arbitrar mecanismos que garanticen la autenticidad del contenido de la historia y de los cambios operados en ella, así como la posibilidad de su reproducción futura. De la aplicación de esta regla y de lo dispuesto en los artículos 4.3 y 4.4 de la LOPD se desprende que será preciso proceder a la supresión completa del dato previamente registrado.

En todo caso, señala Puente Escobar (2004:36), debe aclararse «que el ejercicio de cancelación ha de entenderse referido a la supresión de datos inadecuados de la historia clínica, nunca a una mera solicitud del interesado de que sus datos sean eliminados por su propia voluntad, dado que la Ley 41/2002 exige la conservación de los datos de la historia clínica, no siendo suficiente una mera voluntad contraria del interesado para que proceda la supresión».

La posibilidad de rectificar los datos de carácter personal, entre los que están los relativos a la salud, es un derecho esencial dada las graves consecuencias que pueden tener los errores en las bases de datos para la vida de las personas, además la Constitución Española

reconoce el derecho a recibir una información veraz (Romero Coloma, 2002).

Algunos ciudadanos han consultado a la Agencia Española de Protección de Datos sobre si tienen derecho a cancelar los datos en la historia clínica de un hospital una vez finalizado el tratamiento en dicho hospital. Asimismo, se pedía información sobre la forma en la que se puede solicitar dicha cancelación y si existe un plazo mínimo para ejercerla. Aunque existe el derecho de cancelación por parte del afectado, este derecho viene limitado en aquellos supuestos en los que exista un deber de conservación de los datos, la Agencia Española de Protección de Datos concluye afirmando «que existen numerosas normas sanitarias que exigen la creación y conservación del historial clínico siempre que se produzca la intervención de las Administraciones Sanitarias con diversos fines. El mantenimiento de la información viene obligado también por las normas penales y civiles para los supuestos de responsabilidad» (Sánchez Carazo, 2000:165).

Las actuaciones contrarias a la LOPD, y en especial, las denegaciones de los derechos de acceso, rectificación y cancelación pueden ser objeto de reclamación ante la Agencia de Protección de Datos (artículo 18 LOPD). Así, el interesado al que se le deniegue total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación podrá ponerlo en conocimiento de la Agencia de Protección de Datos, o en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. El plazo máximo en que debe dictarse la resolución expresa de tutela es de seis meses, contra las resoluciones de la Agencia de Protección de Datos existe la posibilidad de presentar un recurso contencioso-administrativo (APDCM, 2008).

Antes de promulgarse la Ley 41/2002, y habida cuenta de la inconstitucionalidad del artículo 24.2 de la LOPD, había opiniones favorables al derecho del paciente a la cancelación de los datos de salud. Por ejemplo, señala Sánchez Carazo (2000:165) «el magistrado Ramón Sáez piensa que el usuario tiene derecho a que se oculte hasta el dato de que estuvo y fue tratado en un servicio hospitalario».

En este sentido, la Recomendación N.º R (97)5, en el punto 10, defiende que los datos sanitarios deben ser cancelados a petición de la persona interesada o convertirlos en datos anónimos, siempre y cuando no existan intereses legítimos como: la salud pública; la cien-

cia médica y la investigación; las posibles acciones judiciales. En estos casos, el responsable del tratamiento, tomará las disposiciones técnicas necesarias para garantizar la conservación y seguridad correctas de los datos, teniendo en cuenta la vida privada del paciente. En todo caso, el interesado podrá ejercer o defender sus derechos judicialmente.

Hoy en día, sin embargo, a la vista de la Ley 41/2002 y al menos durante el tiempo establecido en el artículo 17.1 de la misma, puede denegarse al paciente el derecho a la cancelación de sus datos de salud. En efecto, aun declarada la inconstitucionalidad de los preceptos que permitía denegar la cancelación de datos, el artículo 16 de la LOPD (justamente sobre el derecho de cancelación), en su apartado 5 establece el mandato imperativo de conservar los datos de carácter personal durante los plazos previstos en las disposiciones aplicables.

Hasta ahora no existía disposición, a excepción de algunas autonómicas, que estableciera plazo alguno de conservación de los datos de salud. Actualmente, con el artículo 17.1 de la Ley 41/2002 cobra a su vez pleno sentido y aplicabilidad el 16.5 de la LOPD. Téngase en cuenta además que, aunque se trate de una limitación al ejercicio de un derecho constitucional, la misma está establecida mediante norma con rango de ley con toda precisión, cinco (5) años desde la fecha del alta. Más dudas suscita la limitación del derecho de cancelación una vez transcurridos los cinco (5) años del artículo 17.1 de la Ley 41/2002, y a pesar de lo dispuesto en el artículo 17.2 (Atela y Garay, 2004).

En atención a lo expuesto, y a modo de resumen de este punto, al menos durante el tiempo establecido en el artículo 17.1 de la Ley 41/2002, puede entenderse que la referida norma ha introducido un límite temporal al ejercicio del derecho de cancelación de datos de salud, de modo que durante ese tiempo se puede denegar la eventual solicitud de cancelación de datos con las excepciones previstas en el artículo 16.2 de la LOPD cuando se trate de datos inexactos o incompletos.

Según lo ya visto, la cancelación de los datos personales relativos a la salud en algunos casos no va a ser posible; por ello es necesario llegar a un punto de encuentro entre los derechos particulares de los interesados y los intereses generales de la población, por lo que hay que intentar encontrar el punto de equilibrio y compaginar los derechos del paciente y los del bien común.

3.5.3 DERECHO DE OPOSICIÓN A LA OBTENCIÓN DE LA INFORMACIÓN SANITARIA

El derecho de oposición consiste en la posibilidad para el afectado de negarse a la continuación del tratamiento de sus datos. El ejercicio de este derecho se refiere a los datos en que, no siendo necesario el consentimiento del afectado para el tratamiento de sus datos de carácter personal (como ocurre respecto de los datos sobre la salud cuando su tratamiento resulte preciso para la prevención o para el diagnóstico médicos, etc.), existan motivos fundados y legítimos para que dicha persona formule su oposición, atendiendo a una circunstancia particular, y siempre que la ley no disponga lo contrario.

No obstante, como afirma Martín - Casallo (2001) citado por Sánchez-Caro y Abellán (2004:50), «en la práctica apenas se darán con relación al dato sanitario supuestos de ejercicio del derecho de oposición, dada la finalidad de curación que, en el último término, busca su tratamiento, incluso de producirse dicha oposición, podría evidentemente ser rechazada en aplicación de un criterio de primacía del derecho a la vida frente al derecho a la intimidad».

3.5.4 OTROS DERECHOS

La impugnación de los actos administrativos o decisiones privadas por los ciudadanos, en la medida en que impliquen una valoración de su comportamiento y cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad (artículo 13 LOPD).

El derecho a ser informado, recabando para tal efecto la información oportuna del Registro General de Protección de Datos (de la correspondiente Agencia de Protección de Datos), de la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

Por último, el derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, sí como las comunicaciones realizadas o que se prevean hacer de los mismos (artículos 14 y 15.1 LOPD).

3.6 EL RESPONSABLE DEL FICHERO EN EL ÁMBITO SANITARIO

La determinación de quién es el responsable del fichero de historias clínicas o de datos sanitarios es de gran importancia porque será éste el obligado a declarar los ficheros, será él ante quien se ejerciten los derechos de acceso, rectificación y cancelación y es también quien va a responder ante la posible infracción que se cometa en este ámbito.

La LOPD señala que el Responsable del Fichero será la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la *finalidad, contenido y uso del tratamiento*.

La Ley 41/2002 procura aportar luces acerca de quién es el responsable del fichero de historias clínicas; el artículo 17.4 establece que la gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que se atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la Unidad de Admisión y Documentación Clínica, encargada de integrar en un solo archivo las historias clínicas. Ahora bien, la custodia de dichas historias clínicas «estará bajo responsabilidad de la dirección del centro sanitario». Por tanto, en los centros sanitarios corresponde al Gerente la responsabilidad del fichero de historias clínicas. En cambio, los profesionales sanitarios que desarrollen su actividad de manera individual son «responsables de la gestión y de la custodia de la documentación asistencial que generen» (artículo 17.5 Ley 41/2002).

La responsabilidad del fichero de historias clínicas que corresponde a la dirección del centro sanitario no tiene que olvidar que la cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será responsabilidad de los profesionales que intervengan en ella, que tienen el deber de cooperar en la creación y mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes (artículos 15.3 y 17.3 Ley 41/2002).

Es conveniente recordar que existen diferencias en la regulación jurídica de protección de datos entre ficheros públicos y ficheros privados, por tanto, entre los ficheros de los servicios sanitarios públicos y de los servicios sanitarios privados. Así, los centros públicos estarán obligados a seguir la legislación más exigente en cuanto la creación, modificación y supresión de ficheros, consecuencia lógica de un con-

junto de ventajas, por ejemplo, la excepción del consentimiento prevista para el tratamiento de datos realizados por los poderes públicos. Mientras que los ficheros de centros públicos sanitarios deben crearse, modificarse o suprimirse a través de una disposición de carácter general y ser publicados en el Diario Oficial correspondiente, los ficheros de los centros sanitarios privados se crean a través de la notificación previa a la Agencia Española de Protección de Datos (artículo 25 LOPD).

Además, si el régimen de infracciones es semejante, no lo es el régimen sancionador. Así, las sanciones para los responsables de ficheros privados son económicas, desde 600 a 60.000 euros por infracciones leves, hasta 300.000 euros por infracciones graves, y hasta 600.000 euros por infracciones muy graves, sanciones que son acumulativas en el caso que concurran varias infracciones distintas.

En cambio las infracciones cometidas por responsables de ficheros públicos lleva aparejada, como señala el artículo 46 de la LOPD, una resolución de infracción administrativa, el establecimiento de medidas para que cesen o se corrijan los efectos de la infracción, notificación al responsable del fichero y a su superior jerárquico, la propuesta de iniciación de actuaciones disciplinarias y la comunicación al Defensor del Pueblo (APDCM, 2008).

Eso no obsta para que el ciudadano pueda ejercer el derecho de indemnización cuando, como consecuencia de una infracción, sufra un daño o lesión en sus bienes o derechos (artículo 19 LOPD). La Agencia de Protección de Datos no impone una sanción económica a un responsable de un fichero público, lo que sí hace con los responsables de los ficheros privados, ya que inicialmente no tiene sentido que una Autoridad Administrativa sancione a otra. La responsabilidad patrimonial del responsable de un fichero de titularidad pública se exigirá, de conformidad con el régimen de responsabilidad patrimonial de las Administraciones Públicas, ante la Jurisdicción Contencioso-Administrativa.

3.7 PRINCIPALES OBLIGACIONES DE LOS CENTROS Y SERVICIOS SANITARIOS PÚBLICOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Los centros y servicios sanitarios trabajan diariamente con datos de carácter personal, estos datos se refieren principalmente a los

usuarios de los servicios, personal que participa en la prestación de los mismos y empleados públicos que se encargan de su gestión, pero también pueden hacer referencia a terceras personas, por ejemplo, a los familiares de los usuarios o a profesionales ajenos a la propia entidad u organización que presta los servicios.

Para que un fichero entre en el ámbito de aplicación de la normativa en materia de protección de datos es necesario que en el mismo se contengan datos de tipo identificativo de las personas, como su nombre, domicilio, teléfono, dirección de correo electrónico, número de la Seguridad Social, número de empleado o número de historia clínica o social (APDCM, 2004).

Pero los datos de carácter personal pueden ser de naturaleza muy diversa, pudiendo agruparse en otros, en los siguientes:

— Datos de carácter identificativo.

— Datos de características personales.

— Datos de circunstancias sociales.

— Datos académicos y profesionales.

— Datos de detalles del empleo.

— Datos de información comercial.

— Datos económico-financieros.

— Datos de transacciones.

De acuerdo con la legislación vigente, los ficheros utilizados por los organismos e instituciones públicas del ámbito de las comunidades autónomas que contengan datos de carácter personal, han de ser creados mediante disposición de carácter general que debe publicarse en el Boletín Oficial con anterioridad a recabar dichos datos, entendiendo por fichero cualquier conjunto organizado de datos de carácter personal, sea cual sea su tipo de almacenamiento, organización o acceso. Esto incluye información personal en soportes manuales, como ficheros de fichas manuscritas o similares, siempre que tengan una estructura que permita el fácil acceso a los datos de una determinada persona (APDCM, 2008).

3.7.1 RECOGIDA Y TRATAMIENTO ADECUADO DE LOS DATOS PERSONALES

El tratamiento de los datos de carácter personal debe cumplir la normativa en materia de protección de datos en todas sus fases, desde la recogida de información, hasta su archivo y mantenimiento, en particular hay que cuidar especialmente la fase de la recogida de la información.

Los datos que se recojan deben ser los adecuados, pertinentes y no excesivos para la finalidad que se pretende. Esto implica que todos los formularios, cuestionarios o pantallas deben ser diseñados cuidando de recabar tan solo aquellos datos que sean estrictamente necesarios.

Es obligatorio que el centro o institución responsable del tratamiento de los datos, informe a los interesados en el momento de la recogida de los mismos sobre sus derechos relativos a sus propios datos personales. En particular, en todos los impresos o formularios de recogida de datos, con independencia del soporte, debe incluir información relativa a los derechos que asisten a los ciudadanos, dónde y cómo ejercerlos.

Los datos de las personas deben estar permanentemente actualizados y se deben cancelar cuando queden obsoletos, esto implica tener procedimientos individualizados de actualización a petición de los interesados, así como procedimientos masivos periódicos de actualización y cancelación de los datos que mantengan información actualizada (APDCM, 2004).

En cualquier fase de tratamiento, las personas que utilizan los datos de carácter personal están obligadas al secreto profesional, es decir, no pueden revelar la información a terceros. Los datos sólo podrán ser comunicados con el consentimiento del afectado, aunque tal consentimiento no es necesario para entregar datos a otras Administraciones Públicas (Comunidad de Madrid, Administración General del Estado) que ejerzan competencias similares, así como en los casos excepcionales que marquen otras leyes, y el caso de peticiones expresas de los jueces, tribunales, Ministerio Fiscal, Defensor del Pueblo, etc.

3.7.2 FACILITAR A LOS CIUDADANOS EL EJERCICIO DE LOS DERECHOS SOBRE SUS DATOS

Cada vecino, empleado público, colaborador, responsable de una empresa, y en general todos los ciudadanos, tiene derecho de acceder, rectificar y cancelar los datos personales propios que obren en poder de un centro o institución prestadora de servicios sanitarios. La Agencia de Protección de Datos de la Comunidad de Madrid (2008:102) establece que:

— El centro tiene la obligación legal de facilitarles el ejercicio de sus derechos. Es recomendable que el sitio web de la Administración responsable del centro o servicio sanitario publique formularios e instrucciones para el ejercicio de estos derechos por parte de los ciudadanos.

— El centro tiene la obligación de informar gratuitamente a un ciudadano en relación con sus propios datos. El responsable del fichero debe resolver la petición del ciudadano en un plazo máximo de un mes a partir de la recepción de la solicitud.

— El centro o servicio sanitario responsable del fichero tiene la obligación si procede de corregir gratuitamente los datos incompletos o inexactos relativos a cualquier ciudadano que lo solicite en un plazo máximo de diez días a partir de la recepción de la solicitud.

— El centro tiene la obligación de cancelar gratuitamente los datos de un ciudadano que así lo solicite, cuando su tratamiento no se ajuste a la ley, por ejemplo, cuando estén tratando datos sin que el correspondiente fichero haya sido declarado e inscrito en el Registro de Ficheros de la Agencia de Protección de Datos. Cancelar significa *bloquear los datos*, manteniéndolos exclusivamente a disposición de las Administraciones Públicas competentes y de los Jueces o Tribunales, y borrándolos cuando hayan prescrito las posibles responsabilidades derivadas del tratamiento.

Existen supuestos en los que no es posible la cancelación de los datos, aun cuando el titular de los mismos así lo pretenda. En el caso de las historias clínicas, la Ley 41/2002 establece la obligación de que en ellas figure toda la información que se considera trascendental para el conocimiento veraz y actualizado del estado de salud del pa-

ciente, por lo que no será posible eliminar datos relevantes al efecto. Además, la misma norma establece que la documentación clínica debe conservarse para la debida asistencia al paciente durante el tiempo adecuado a cada caso, y como mínimo cinco (5) años contados desde la fecha de alta de cada proceso asistencial.

3.7.3 ELABORACIÓN E IMPLANTACIÓN DE MEDIDAS DE SEGURIDAD: EL DOCUMENTO DE SEGURIDAD

Con carácter general, el centro o institución responsable del fichero tiene que implantar las medidas de seguridad adecuadas al grado de protección de cada uno de los ficheros con datos de carácter personal de que disponga, incluyendo: la designación de un responsable de seguridad, al que debe dotarse de autoridad suficiente; la asignación de medios materiales (personal, presupuesto, equipos informáticos, etc.); definir una política de seguridad incluyendo obligaciones y recomendaciones para el personal del centro o servicio sanitario; y la concienciación de los usuarios, mediante notificaciones internas, sesiones de difusión o formación sobre protección de datos personales y sobre la política de seguridad adoptada por el centro o servicio sanitario (APDCM, 2008).

El centro o servicio sanitario debe elaborar un Documento de Seguridad cuyo cumplimiento será obligatorio para todo el personal que tenga acceso a datos personales y a las aplicaciones informáticas y sistemas de información correspondientes, que debe incluir como mínimo:

— Ámbito de la aplicación.

— Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad: nivel básico, medio o alto.

— Funciones y obligaciones del personal.

— Estructura de los ficheros con datos de carácter personal, incluyendo una descripción del sistema de información.

— Procedimiento de notificación de incidencias.

— Procedimiento de realización de copias de respaldo.

3.7.4 GARANTIZAR LA PROTECCIÓN DE DATOS PERSONALES EN LOS CONTRATOS CON TERCEROS

En ocasiones, los centros o instituciones públicas prestadoras de servicios sanitarios contratan o acuerdan mediante convenio con terceros la prestación de determinados servicios que requieren el tratamiento, por parte de aquellos, de datos personales de empleados, usuarios de los servicios, pacientes ingresados, familiares u otros ciudadanos. Ejemplos típicos de este supuesto son la externalización *(outsourcing)* de la gestión del fichero de historias clínicas en soporte no informatizado o la contratación de la elaboración de un *mailing* a determinados pacientes o usuarios de un centro o servicio sanitario.

Es obligación del responsable del fichero garantizar que los contratos firmados a estos efectos recojan las garantías precisas sobre el tratamiento de datos de carácter personal recogidos en sus ficheros, para tal efecto la Agencia Española de Protección de Datos propone la utilización o adaptación de cláusulas tipo al caso concreto. Es importante resaltar que el centro o servicio sanitario debe comunicar a la Agencia de Protección de Datos cualquier contrato que incluya el tratamiento de datos de carácter personal por parte de un tercero, con anterioridad a la firma del mismo (APDCM, 2008).

En cualquier caso, no es preciso un contrato o convenio específico de protección de datos sino que se cumple con la obligación incluyendo las cláusulas de protección de datos, en los términos del artículo 12 LOPD, dentro del contrato de prestación del servicio u obra, en el convenio o en el pliego de prescripciones administrativas o técnicas.

3.8 UNA POSIBILIDAD DE AUTORREGULACIÓN: LOS CÓDIGOS TIPO

La LOPD contempla la posibilidad de que los responsables de los ficheros y tratamientos puedan ampliar o adecuar a las peculiaridades del sector en el que operan, las previsiones normativas sobre protección de datos personales, no obstante, habrán de respetarse plenamente.

En este sentido, como afirma Rubí Navarrete (2000) citado por Sánchez-Caro y Abellán (2004:62), los código tipo «son códigos deontológicos o de buena práctica profesional elaborados por los responsables del tratamiento de datos personales para ampliar o facilitar el cumplimiento de las obligaciones establecidas en la normativa sobre protección de datos personales, incrementar las garantías de los ciudadanos y el ejercicio de sus derechos, reforzar las estructuras organizativas y técnicas en el tratamiento de aquellos y, en particular, las medidas de seguridad; o contemplar procedimientos específicos para la tutela de los principios y derechos exigibles en esta materia».

Los código tipo deben ser depositados o inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos y, cuando proceda en el de la Comunidad Autónoma correspondiente, que podrán denegar la inscripción de los mismos cuando consideren que no se ajustan a las disposiciones legales y reglamentarias sobre la materia de protección de datos personales. Su aplicación al campo sanitario es perfectamente posible, tanto en el ámbito privado como en el público, ya que la regulación de la LOPD sobre esta materia es flexible y permite que puedan adaptarse a las necesidades de una sola empresa o de la totalidad o parte de un sector empresarial o profesional, sin distinción del carácter público o privado del responsable del fichero (Rubí Navarrete, 2004).

No obstante, como señala la Agencia Española de Protección de Datos, la adhesión al código en ningún caso modifica el régimen de obligaciones establecido por la LOPD y resto de normativa vigente en materia de protección de datos. Por ello, los adheridos al código tipo previamente cumplirán todas las obligaciones legales establecidas, con especial consideración a las que se refieren a la notificación al Registro General de Protección de Datos de los ficheros existentes y la aplicación de las medidas de seguridad correspondientes, según Reglamento de desarrollo de la LOPD (Real Decreto 1790/2007).

Estos Código Tipo deben tener un valor añadido, que puede consistir, bien en establecer un sistema de garantías, más allá de lo exigible legalmente, o bien adaptar la normativa de protección de datos a las peculiaridades específicas de un sector, de forma que el código tipo cumple una función pedagógica que facilita el cumplimiento de la LOPD.

El Código Tipo debería empezar partiendo del análisis de los puntos críticos que tiene un sector en el tratamiento de datos personales, por ejemplo, en el ámbito sanitario hay que hacer una reflexión sobre cuál es el primer punto crítico específico del tratamiento de los datos personales, así cuando un paciente llega al servicio de Admisión, se le puede ofrecer información sobre aspectos muy variados para que decida la que puede suministrarse el hecho de que está efectivamente ingresado en esa institución o que no lo está, el que se pueda facilitar información sobre si está ingresado, pero no en qué servicio está ingresado, porque eso puede permitir obtener información adicional. Es decir, hay que ir haciendo repaso de todos los tratamientos de datos que se producen en el sector, analizar los puntos que son críticos, y tratar de buscar soluciones específicas, adaptadas a esa situación, en las previsiones de la LOPD.

Los Código Tipo, además, tienen que ofrecer soluciones al particular porque el último destinatario del código tipo es el ciudadano. Al responsable del fichero le son de utilidad porque permite estandarizar su conducta, pero el último destinatario es el afectado. Por tanto, tiene que tener una terminología comprensible, no es necesario que un código tipo reproduzca sistemáticamente conceptos o términos legales. El código tipo tiene que tener mecanismos internos de control y mecanismos reparadores. Estos mecanismos reparadores en los código tipo es para los casos en que se produzca un incumplimiento del código, muchas veces tienen una naturaleza, no económica, como por ejemplo, la amonestación, o el comprometerse a hacer público los incumplimientos que se han producido.

Aunque no tengan ese valor económico, son previsiones muy importantes, porque, por ejemplo, si un centro sanitario se adhiere a un código tipo, que normalmente va acompañado de un sello de calidad que acredite que se cumplen con rigor las previsiones de la LOPD, y en un momento determinado, se aprecia un incumplimiento, estando ésta previsto que se puede hacer público ese incumplimiento, la imagen del centro sanitario puede sufrir un deterioro tan importante, que quizás tenga consecuencias más graves que la del mero hecho de imponer una multa. Por eso en este tipo de códigos, normalmente las sanciones internas que se prevén, suelen ser de esta naturaleza (Rubí Navarrete, 2004).

Los Códigos Tipo establecen una serie de pautas interpretativas de las disposiciones de la LOPD, dirigidas a implantar un régimen homogéneo de protección de datos personales en el seno de sus respectivos centros asociados, y contienen modelos de impresos de información y formularios para el ejercicio de los derechos de acceso, rectificación, etc. de los usuarios, así como para otras cuestiones relacionadas con la materia. Además, prevén mecanismos propios de depuración interna de responsabilidades, adicionales a los dispuestos en la LOPD, con sanciones que pueden conllevar la pérdida de la condición de socios para los centros o establecimientos infractores.

3.9 TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES DE SALUD

En el mundo globalizado en el que vivimos, se producen con frecuencia intercambios de datos personales entre entidades que manejan datos de salud, que se encuentran en diferentes países y cuya normativa de protección de datos es también distinta, lo que en determinadas ocasiones puede hacer perder a los ciudadanos de la Unión Europea (UE) el elenco de garantías que sobre el control de sus propios datos tienen reconocidos en sus países de origen, donde las disposiciones internas en esta materia se encuentran armonizadas dentro del marco de la Directiva 95/46/CE sobre protección de datos (Remolina Angarita, 2013).

Por esta razón, en España la LOPD sienta el principio general de que no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal, que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable, salvo que además de haberse observado lo dispuesto en la citada LOPD, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, una vez comprobada la existencia de garantías adecuadas.

A la regla general anterior, la LOPD opone una serie de excepciones entre las que se encuentran los supuestos en los que el afectado haya dado su consentimiento inequívoco a la transferencia prevista, o que la misma sea necesaria para la prevención o diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la legisla-

ción de servicios sanitarios (por ejemplo, en ciertos casos de práctica de la telemedicina, o de utilización de un seguro médico en otro país) (Sánchez-Caro y Abellán, 2004).

No obstante, con el fin de clarificar qué debe entenderse realmente por una transferencia internacional de datos personales, se debe acudir a la Instrucción 1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos, donde se matiza que este concepto abarca dos realidades distintas: por un lado, son transferencias internacionales de datos aquellas en las que se produce una comunicación de datos a un tercero fuera de España que actúa por cuenta propia decidiendo sobre la finalidad del tratamiento (que es por tanto, el responsable del tratamiento). Son los casos en que la comunicación de datos entre el cedente y el cesionario se produce para el cumplimiento de los fines directamente relacionados con las funciones legítimas de uno y otro (por ejemplo, la utilización, en España, de una tarjeta de asistencia sanitaria cuya entidad proveedora tenga su centro de operaciones en otro país).

Y por otro lado, también se califican como transferencias internacionales de datos, aquellas que no implican una comunicación en el sentido indicado anteriormente, sino que el tercero situado fuera de España va a actuar como mero encargado del tratamiento del transmisor y por cuenta de éste último (por ejemplo, un centro hospitalario español subcontrata con otra entidad localizada en el extranjero la realización de determinados actos de administración y gestión de las historias clínicas electrónicas que están bajo su custodia).

En este sentido, como sostiene la profesora Sancho Villa (2003:23) citada por Sánchez-Caro y Abellán (2004:80), «una transferencia internacional de datos personales relevante para el ordenamiento español, es aquella que supone la salida física al extranjero de datos personales que se encuentran en territorio español, al margen de que dicha transmisión suponga también la salida jurídica en el sentido de la pérdida de competencia de la ley española (no se produce la salida jurídica, aunque sí física, cuando el receptor de los datos establecidos en el extranjero es un mero encargado). También es indiferente a efectos conceptuales que la transferencia se produzca entre sujetos de Derecho público o privado».

Por tanto, con carácter general (dejando a salvo los supuestos exceptuados por la ley), si la finalidad del tratamiento de datos persona-

les va a conllevar su transferencia internacional, será necesaria la concurrencia de dos consentimientos por más que se supongan, uno para la recogida de datos y otro para la transferencia de los mismos, pudiendo incluso coexistir la necesidad de un tercer consentimiento si la transferencia se desea llevar a efecto a un país que no garantiza un nivel de protección adecuado y se quiere hacer sin contar con la autorización del Director de la Agencia Española de Protección de Datos (Sancho Villa, 2003).

3.10 DATOS MÉDICOS O DE SALUD

A pesar de no existir duda alguna sobre el carácter personal de los datos relativos a la salud y de la importancia y trascendencia de los mismos, hay que señalar que se trata de un concepto aún no definido por la legislación española, ni la derogada Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (en adelante LORTAD), ni la vigente Ley Orgánica de Protección de Datos de Carácter Personal (en adelante LOPD), ni la Ley 41/2002 Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica entran a definirlo, como tampoco lo hacen las normas dictadas en desarrollo de las mismas. Por ello, el análisis del indicado concepto se realiza utilizando como criterio la definición ofrecida por el artículo 1 de la Recomendación Número 5[21], así como la definición que la LOPD ofrece de dato de carácter personal, los datos médicos se definen como «aquellos datos personales relativos a la salud de un individuo, comprendiendo igualmente los que tengan una clara y estrecha relación con la salud y los datos genéticos».

Dato médico comprende todos aquellos datos de carácter personal que estén relacionados con la salud de una persona física. Evidentemente, desde el momento en el que no exista dicha conexión o víncu-

---

[21] Recomendación Número 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados Miembros sobre Protección de Datos Médicos. Se debe tener cuidado de no confundir el Consejo de Europa con el Consejo Europeo ni con el Consejo de la Unión Europea. El Consejo de Europa es una organización política europea establecida tras la Segunda Guerra Mundial que no tiene relación con la Unión Europea.

lo entre los datos y su titular, no se podrá hablar de dato médico (Jañez *et al.,* 2002).

Para Sánchez Carazo (2000:112) los datos de salud «son todos aquellos datos de carácter personal que indiquen la situación de salud o enfermedad de un individuo». Asimismo, señala que se deben incluir los antecedentes médicos, el diagnóstico, los procedimientos realizados, el tratamiento, el pronóstico relativo a su salud física o psíquica, o la información genética, y los datos administrativos de los centros sanitarios.

Murillo de la Cueva (1997) entiende que el concepto de datos relativos a la salud han de incluirse los de carácter médico, pero también los que mantengan conexión con fines relacionados con la salud, sean tratados en el ámbito de la salud pública, en seguros de enfermedad o en actividades científicas o estadísticas.

Fuera del ámbito europeo, resulta de interés mencionar lo recogido al respecto por Sánchez-Caro y Abellán (2002) de la ley de confidencialidad de los datos sanitarios estadounidenses[22], que contempla un concepto de datos sanitarios muy amplio, que abarca incluso los aspectos económicos relacionados con la prestación de la asistencia sanitaria. De esta forma en la citada ley se definen los datos médicos como toda información, bien oral, bien grabada en cualquier forma o medio que haya sido creada o recibida por un proveedor de servicios de salud, plan de salud, autoridad pública de salud, empresario, compañía de seguros de vida, escuela o universidad, o entidad encargada del tratamiento de datos de salud; que se refiera a la salud física o mental, o a alguna circunstancia de la salud de una persona en el pasado, presente o futuro; a la provisión de cuidados de salud personales; o el pago de los servicios de salud que hubiera realizado una persona en el pasado, que se lleve a cabo en el presente o vaya a realizarse en el futuro.

Señala De Miguel Sánchez (2004) que se debe buscar un concepto amplio y expansivo de dato médico, que merezca una consideración plenamente positiva, pues una definición pormenorizada podría dejar

---

22 *Standar for Privacy of Individually Indentifiable Health Information,* del *Department of Health and Human service*, ley vigente en Estados Unidos de América desde 2001.

fuera informaciones que inciden sobre la salud de la persona y que de no verse expresamente contempladas podrían generar situaciones de indefensión y de potencial agresión contra los derechos de los particulares y dificultar el control de éstos sobre unos datos de carácter personal, que como se ha aceptado de forma común son especialmente sensibles.

Desde el punto de vista del Consejo de Europa, de la misma Agencia Española de Protección de Datos, y por supuesto, de los tribunales a la hora de decidir sobre estas cuestiones (2007). Se define a los datos médicos como aquellos referentes a la salud de una persona, ya sea pasada, presente o previsiblemente futura, o también los referidos a posibles adicciones del sujeto objeto de observación; también lo son aquellos datos meramente administrativos (el nombre, su teléfono o dirección) que estén ubicados físicamente en las dependencias sanitarias, o no estándolo ahí, dependan de ésta (pueden estar alojados en un servidor situado físicamente en otro lugar, fuera de la consulta o clínica, pero controlado por ésta).

En consecuencia, siendo lo más extensos posible para poder abarcar un concepto amplio y expansivo de qué se debe entender por datos médicos o de salud, quedaran comprendidos, todos aquellos datos que tienen que ver con el cuerpo humano, como la sexualidad, la raza, el código genético, los antecedentes familiares, los hábitos de vida, de alimentación y consumo; los datos antropométricos como peso, talla y edad; las enfermedades actuales, pasadas o futuras previsibles, bien sean de tipo físico o psíquico; las informaciones relativas al abuso de alcohol o al consumo de drogas[23]; los datos meramente administrativos de los centros sanitarios; y los aspectos económicos relacionados con la prestación de la asistencia sanitaria. En definitiva

---

[23] Ver apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, hecho en Estrasburgo y ratificado por España el 27 de enero de 1984. En dicho apartado se definen los datos de carácter personal relativos a la salud como «las informaciones concernientes a la salud pasada, presente y futura, física y mental de un individuo» pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. Añade el citado apartado 45 que «debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas».

lo que se pretende es abarcar todos los datos que de alguna forma se refieran a la salud tanto de individuos con buena salud, enfermos o fallecidos.

Por lo tanto, se puede afirmar que los datos médicos son un tipo de dato personal, caracterizados por estar referidos a la salud de las personas físicas. Además de conformidad con el artículo 7 de la LOPD, los datos de salud tienen una consideración de datos especialmente protegidos, por lo que se exigen criterios más estrictos para su uso, tratamiento y cesión, así como medidas de seguridad que deben ser adoptadas en los ficheros donde se contengan dichos datos.

3.11 LA LEY 41/2002 BÁSICA REGULADORA DE AUTONOMÍA DE LOS PACIENTES Y DE LOS DERECHOS DE INFORMACIÓN Y DOCUMENTACIÓN CLÍNICA

3.11.1 EL DERECHO A LA INTIMIDAD

El derecho a la intimidad se ve implicado de forma específica en las relaciones médico-paciente, el enfermo debe confiar en el médico, y frecuentemente le confía datos reservados que no comunicaría a otros. Señala Rodríguez López (2004:107) que «le desvela parte de su intimidad, pero a los solos efectos de su terapia, no le hace partícipe de sus intimidades indiscriminadamente, sino que se trata de una renuncia a su intimidad condicionada a un fin: su curación».

El derecho a la intimidad del paciente supone la obligación del profesional sanitario de mantener en secreto cualquier información proporcionada por su paciente en el ámbito estricto de la relación médico-paciente, no pudiéndosela revelar a un tercero sin su consentimiento específico, o sin que se ampare en una causa legal expresa que le exima del deber de secreto.

La confidencialidad deriva del derecho a la intimidad, que como ha quedado expuesto a través de su régimen legal, protege contra una serie de intromisiones no deseadas en el ámbito de la salud. Intimidad y confidencialidad son dos conceptos muy próximos, pero que difieren en algunas de sus formulaciones. En efecto, la intimidad se refiere

a la limitación del acceso al propio cuerpo o a la mente, como ocurre a través del contacto físico de la revelación de pensamientos o de sentimientos. La confidencialidad, por el contrario, se refiere a la comunicación de información personal de una persona a otra, cuando se espera que la persona que recibe la información, como sucede en el caso de los profesionales sanitarios, no revelará habitualmente la información confidencial a una tercera persona (De Lorenzo y Montero, 2003).

También el Tribunal Constitucional ha tenido ocasión de pronunciarse al respecto, al hablar de la particularidad de la relación que se establece entre el profesional de la medicina y el paciente, basada firmemente en la confidencialidad y discreción y de los diversos datos relativos a aspectos íntimos de su persona que con ocasión de ella suelen facilitarse.

El artículo 18.1 de la Constitución española establece: «Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen». El Tribunal Constitucional llegó a considerar el citado derecho como un poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en el esfera íntima de la persona y la prohibición de hacer uso de lo así conocido.

La Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho de Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, establece en su artículo 2:

1. «La protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales, atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma y su familia.

2. No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por la ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso».

En este sentido, el artículo 10.3 de la Ley General de Sanidad establece el derecho de los pacientes a la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público.

En este sentido conviene recordar que, la LOPD califica a los datos relativos a la salud de los ciudadanos como datos especialmente protegidos, estableciendo un régimen riguroso para su obtención, custodia y eventual cesión, como se vio precedentemente. Importa destacar que el consentimiento debe ser expreso, sin que la ley determine la obligatoriedad de la escritura, aunque a efectos de la llamada prueba preconstituida es muy aconsejable que así se haga, en previsión de problemas ulteriores. Por otra parte, la LOPD establece que el consentimiento que se presta al efecto, es decir, con un objetivo determinado fuera del mismo, el consentimiento deja de surtir efectos.

Por ello es obvio que la Ley 41/2002 señale que toda persona tiene derecho a que respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la ley. Los centros sanitarios deben adoptar las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes (artículo 7.1 y 7.2 Ley 41/2002).

3.11.2 LOS PRECEDENTES DE LA LEY 41/2002

Los derechos de los pacientes son un factor fundamental de las relaciones clínico-asistenciales; ello se evidencia, al menos en el terreno material, por el interés que han demostrado, generalmente en su protección, casi todas las organizaciones internacionales con competencias en la materia. Entre los textos internacionales que se han ocupado de aspectos relacionados con los derechos de los pacientes se puede mencionar, por su importancia o repercusión:

— El Código de Nuremberg, de 1947, que reconoce el derecho de los pacientes a su libre autodeterminación. Su primer artículo comienza afirmando que «el consentimiento voluntario del sujeto es absolutamente esencial».

— La Declaración Universal de los Derechos Humanos, de 1948, recoge expresamente el principio de la dignidad humana, entendiéndolo como fundamento último de los derechos humanos. Este texto es una referencia explícita de los principios básicos de la Ley 41/2002.

— La Declaración sobre Promoción de los Derechos de los Pacientes en Europa, promovida en 1994 por la Oficina Regional para Europa de la Organización Mundial de la Salud (OMS).

— La Directiva 95/46/CE, de 24 de octubre, en ella se trata la defensa de la intimidad relativa a la información relacionada con la salud de los ciudadanos europeos. En el citado texto también hace referencia a otros intereses generales, como los estudios epidemiológicos, las situaciones de riesgo grave para la salud de la colectividad, la investigación, los ensayos clínicos que, cuando estén incluidos en normas de ley, pueden justificar una excepción motivada a los derechos de los pacientes.

— La Recomendación N.º R(97)5 del Consejo de Europa, de 13 de febrero de 1997, relativa a la protección de datos médicos, afirma que los datos médicos deben recogerse y procesarse con el consentimiento del afectado, e indica que la información puede restringirse, si así lo dispone una ley, y constituye una medida necesaria por razones de interés general.

— El Convenio del Consejo de Europa para la Protección de los Derechos Humanos y la Dignidad del ser Humano respecto de las Aplicaciones de la Biología y la Medicina (Convenio de Oviedo), suscrito el 4 de abril de 1997, y que entró en vigor en España el 1 de enero de 2000. Este Convenio es de gran importancia ya que es el primer instrumento internacional con carácter vinculante para los países que los suscriben. En el artículo 1 se afirma como primer objetivo de la norma la protección del ser humano en su dignidad. En el texto se trata, explícitamente, el reconocimiento de los derechos de los pacientes, entre los que resalta el derecho a la información, el consentimiento informado y la intimidad de la información relativa a la salud de las personas.

— La Carta de los Derechos Fundamentales de la Unión Europea del año 2000, redactada en Niza el 7 de diciembre; en el texto se establecen los principios recogidos en la Ley Básica: dignidad de la persona, respeto a la autonomía e intimidad del sujeto. En el artículo 8 se expresa que la protección de datos es un derecho de todo ciudadano (López Guzmán, 2004).

La Ley 41/2002, de 14 de noviembre completa la Ley General de Sanidad, reforzando y otorgando un trato especial al derecho de au-

tonomía del paciente. La nueva ley deroga los apartados 5, 6, 8, 9 y 11 del artículo 10; el apartado 4 del artículo 11; y el artículo 61 (única disposición que hasta ese momento se ocupaba de la documentación clínica) de la Ley General de Sanidad; considera también los aportes de las leyes autonómicas promulgadas hasta ese momento[24]. A su vez, que tiene en cuenta lo expuesto en el Convenio de Oviedo sobre consentimiento informado, y dedica una especial atención a la documentación clínica generada por los centros asistenciales.

Es importante destacar el carácter de norma básica que tiene la Ley 41/2002, en virtud de la distribución de competencias establecida por la Constitución española de 1978, corresponde al Estado la competencia normativa básica en materia de sanidad y a las autonomías el desarrollar las normas dictadas por el Estado, no pudiendo existir normas contrarias a las que el Estado sustenta.

No todas las leyes autonómicas aparecidas de forma previa a la publicación de la Ley 41/2002 partían de iguales premisas, de ahí que se pueda calificar como una ley oportuna para evitar la disparidad a que habían dado lugar los textos autonómicos, en aspectos básicos y comunes a todos los ciudadanos.

3.11.3 LOS PRINCIPIOS GENERALES DE LA LEY 41/2002

En la Ley 41/2002, el hecho de que el legislador estatal se haya fijado en los principios que se harán mención y se los haya plasmado en esta regulación, no se debe a una originalidad suya, porque esos mismos principios y similar regulación se encuentran en las leyes autonómicas que sobre esta materia se han promulgado con anterioridad a esta ley y en las leyes estatales de países del entorno cultural español, como Francia o Estados Unidos. Todas ellas responden a una preocupación común por la defensa de los derechos individua-

---

[24] Ley de Derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica, de Cataluña (Ley 21/2000, de 29 de diciembre); la Ley reguladora del consentimiento informado y de la historia clínica de los pacientes de Galicia (Ley 3/2001, de 28 de mayo); o la Ley sobre derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica de Navarra (Ley Foral 11/2002, de 6 de mayo).

les, en concreto de los derechos del paciente, que se viene poniendo de relieve desde hace años en organismos internacionales desde donde se han ido trazando las líneas generales que esta ley obedece (San Julián, 2004).

El artículo 2 de la Ley 41/2002, lleva por título «Principios básicos» y se desglosa en siete apartados:

1. «La dignidad de la persona humana, respeto a la autonomía de su voluntad y su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y documentación clínica.

2. Toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes o usuarios. El consentimiento, que debe obtenerse después de que el paciente reciba una información adecuada, se hará por escrito en los supuestos previstos en la ley.

3. El paciente o usuario tiene derecho a decidir libremente, después de recibir la información adecuada, entre las opciones clínicas disponibles.

4. Todo paciente o usuario tiene derecho a negarse al tratamiento, excepto en los casos determinados en la ley. Su negativa al tratamiento constará por escrito.

5. Los pacientes o usuarios tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria.

6. Todo profesional que interviene en la actividad asistencial está obligado no sólo a la correcta prestación de sus técnicas, sino al cumplimiento de los deberes de información y de documentación clínica, y al respeto de las decisiones adoptadas libre y voluntariamente por el paciente.

7. La persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar reserva debida»

Este artículo contiene un apartado en el que plasma el principio eje y en los restantes una serie de derechos en los que se concreta y despliega, al mismo tiempo, ese principio. El apartado primero es el

que recoge el principio eje, que se podría reelaborar así: «la dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad que se desarrolla en el ámbito médico relativa a información y documentación clínica». Por tanto, este principio vincula a toda persona que participa en la prestación de servicios médicos, a todo el personal sanitario, desde los celadores y auxiliares, pasando por las enfermeras/os, hasta el colectivo médico; si bien estos últimos son, junto con el titular del centro médico en que se lleva a cabo dicha actividad, la cabeza visible y máximos responsables del cumplimiento de los deberes en que este principio se plasma (Corbella Duch, 2006).

Constantemente se ha venido hablando de derechos, pero no se debe olvidar que de esta Ley 41/2002 se desprenden tanto derechos como deberes, así lo recoge el propio título de la ley. Para San Julián (2004:69) los derechos/deberes que derivan de esta ley tanto para pacientes como para el profesional sanitario son:

— *Derivados del respeto a la dignidad de la persona y a su autonomía:* El personal sanitario tiene el deber de informar adecuadamente al paciente, de contar con su consentimiento informado y de respetar lo que éste decida, mientras que el paciente, en virtud de su autonomía, tiene el derecho a decidir a la vista de lo que se le ha informado. Es decir, que sobre su derecho básico a ser informado se asienta otro derecho, el de consentir, de ahí la interconexión entre ambos derechos, de manera que sin información, o con una información incorrecta o incompleta no se pueda manifestar un consentimiento informado.

— *El respeto a la dignidad de la persona y a su intimidad:* El paciente tiene deber de facilitar sus datos que sean precisos o colaborar en su atención, mientras que el personal sanitario tiene el deber de custodiar debidamente esos datos y mantener la discreción en relación a los mismos. En definitiva el propio artículo 2.6 resume lo que serían los deberes que esta ley impone al profesional sanitario, de tal manera que probablemente una de las grandes novedades de esta ley es que a partir de ahora se puede decir que esos deberes, con el de informar a la cabeza, pasan a ser parte integrante y esencial de la *lexartis*.

La Ley 41/2002 habla de derechos y deberes, lo cual lleva a pensar en un primer momento que se trata de derechos y deberes tanto de los

pacientes como de los médicos, pero realmente de la redacción de esta ley se desprende que cuando se habla de derechos el titular es siempre el paciente, y cuando aparecen los deberes el sujeto obligado es el médico o el personal sanitario, ya que cuando algún deber hace referencia al paciente las consecuencias de su infracción no son las mismas.

A la luz de lo recogido en este artículo 2 de la Ley 41/2002 se puede hacer algunas apreciaciones, en primer lugar destacar que los derechos y deberes que aparecen recogidos en esta ley no son nuevos sino que se corresponden con el desarrollo de derechos ya existentes o bien se encontraban recogidos en Códigos éticos o de Deontología profesional, o bien plasmados en normas jurídicas, pero recogidos con tal amplitud y ambigüedad que resultaba difícil saber el alcance de su vinculación, o por el contrario, plasmados en normas sectoriales tan específicas que hacían que estos derechos sólo fueran exigibles en éste ámbito. De tal manera que la novedad principal de esta ley señala San Julián (2004:72) «no está en los derechos en sí sino en el paso que se da, en relación a alguno de ellos, de deber ético a deber jurídico concreto, con las consecuencias que ello tiene de exigibilidad y responsabilidad».

Aunque la Ley 41/2002 no contiene ningún régimen sancionador de las conductas que vulneren tales derechos, no se puede olvidar que esta norma está inserta y debe ser completada con el resto del ordenamiento, de modo que son de aplicación las normas sancionadoras administrativas, las específicas contendidas en la LOPD, así como el régimen general de responsabilidad civil previsto en el Código Civil y la Ley de Responsabilidad Patrimonial de la Administración, e incluso se puede acudir en algunos casos al Código Penal, por ejemplo, en el caso tipificado en el artículo 197 como delito de descubrimiento y revelación de secretos.

3.11.4 EL NUEVO ENFOQUE DE LA LEY 41/2002

La Ley 41/2002 supone un nuevo peldaño en el proceso de cambio que viven los agentes de la salud a favor de los pacientes que han adquirido un papel protagonista y decisivo en las relaciones sanitarias. Este proceso ha sido descrito por algunos como la implantación de un modelo de autonomía sobre uno anterior de beneficencia, también llamado paternalismo.

3.11.4.1 El protagonismo del paciente

El cambio de la situación del paciente en relación con el médico, enfermero o farmacéutico ha planteado, como era de esperar, una desestabilización de los vínculos que tradicionalmente existían entre estos sujetos. Desde los distintos ámbitos se ha trabajado buscando volver al equilibrio necesario para lograr una satisfactoria asistencia sanitaria. La Ley 41/2002 viene a suponer una gran ayuda en este proceso de cambio social porque, aunque en una primera lectura ofrece la impresión de decantarse excesivamente por los derechos del paciente, cuando se profundiza en el texto se puede vislumbrar que lo que hay detrás es un intento de ponderación de derechos y deberes, con la pretensión de encontrar el equilibrio entre los intereses de profesionales sanitarios y pacientes.

López Guzmán (2004:28) establece que «en el difícil equilibrio entre pacientes y sanitarios se detecta un paulatino cambio de valores, se pasa del predominio de la jerarquía al de libertad; del de lealtad al de opción; y del de deber al de derecho. Así, el paciente puede pasar de un respeto ancestral a la figura del médico, de un compromiso con lo decidido y de la asunción de un deber con el facultativo, a una situación contraria de individualismo más o menos extremo». A este respecto, conviene señalar que los citados valores no se pueden presentar de forma contrapuesta, el equilibrio de todos es necesario para establecer un proyecto valioso en el que se respete a los integrantes del proceso asistencial.

Así, por ejemplo, pueden verse superadas las figuras extremas de paternalismo médico o de imposición de derechos por parte del paciente, a través de la visión relacional del bien, en que la terapia no es adoptada solitariamente por el enfermo, sino que es fruto del diálogo y de la interrelación entre dos sujetos, el sanitario y el paciente.

3.11.4.2 La información

En esta materia es preciso recordar que, cuando se habla del deber de información clínica, la doctrina científica y la jurisprudencia habían venido insistiendo en que el deber de información clínica presenta una doble vertiente según su función. Por un lado, está el deber de información como presupuesto del consentimiento informado, y por

otro, el deber de información como presupuesto indispensable para el tratamiento óptimo; ambas clases de información se contienen tras la entrada en vigor de la Ley 41/2002 en la única categoría de la información clínica (Corbella Duch, 2006).

La Ley 41/2002 supone una verdadera novedad en lo que respecta al diálogo, el intento de potenciar y recuperar el auténtico encuentro entre dos sujetos, restando importancia la burocracia que estaba estropeando el proceso asistencial. Así, en el artículo 4 se indica que la información «como regla general, se proporcionará verbalmente dejando constancia en la historia clínica», y en el artículo 8.2 se especifica que «el consentimiento será verbal por regla general». No obstante, no hay que olvidar que se tiene que hacer constar en la historia clínica que se ha obtenido. Cabe preguntar si esta medida está orientada a evitar unos trámites innecesarios o tiene carácter defensivo para las posibles quejas ulteriores por parte del paciente. Este puede ser uno de los puntos que más controversia legal suscite en el futuro, ya que la percepción de hasta dónde ha llegado el consentimiento oral estará siempre acompañada de elementos subjetivos (López Guzmán, 2004).

El problema de la información clínica no es tanto un problema legal como un problema de cambio de paradigma de las relaciones sanitarias, del paternalismo tradicional a la participación en la toma de decisiones sanitarias. Señala De Lorenzo y Montero (2003:27) que «el aprendizaje de esta nueva relación exige cambios de mentalidad en los profesionales que no se consiguen sólo a golpe de ley, sino mediante la implantación de medidas educativas, formativas y de participación de los profesionales».

3.11.4.3 **De la información completa a la comprensible**

La información como derecho autónomo del paciente se configura como aquél derecho a conocer los datos disponibles sobre su salud y estado físico en términos adecuados, comprensibles y suficientes, así como sobre la forma de preservarla, cuidarla y mejorarla.

La Ley General de Sanidad establecía que la información debía ser completa, en cambio, el artículo 4.2 de la Ley 41/2002 señala «la información clínica se comunicará al paciente de forma comprensible y

adecuada a sus necesidades y le ayudará a sus decisiones de acuerdo con su propia y libre voluntad». La expresión completa no es viable si se toma en forma literal, ya que es totalmente incompatible con la práctica médica, en cambio, que sea comprensible y adecuada se ajusta más a la realidad. Hay que recordar que en este aspecto la Ley 41/2002 ha seguido la línea planteada por el Convenio de Bioética de Asturias y la Declaración de Bioética de Gijón (López Guzmán, 2004).

Esta información deberá proporcionarse en términos comprensibles para el paciente, o para las terceras personas a las que deba proporcionarse la misma, lo que significa que debe adaptarse a su nivel intelectual y cultural respectivo, evitando en lo posible el recurso al lenguaje técnico. Como se ha dicho, resulta controvertida la utilización del lenguaje técnico en la información, así como de los porcentajes numéricos en la expresión de riesgos. Si bien es cierto que estos últimos otorgan, por una parte, precisión a la información, por otra vuelven más incompresible para los pacientes porque no tienen costumbre de manejo de lenguajes probabilísticos (Corbella Duch, 2006).

Aun cuando el legislador ha atribuido a los profesionales sanitarios la responsabilidad de la información al paciente, las Administraciones e instituciones sanitarias deben ser conscientes también de sus responsabilidades respecto a la información clínica. Deben impulsar la elaboración y difusión de guías y protocolos de consentimiento informado, que permitan a los profesionales conocer las pautas claras de actuación en este campo, un modelo básico de documento escrito de consentimiento de estructura abierta puede ser útil en el alcance de este objetivo. Deben, asimismo, facilitar medios de formación de los profesionales en este sentido, incluir el derecho a la información en los programas de formación continuada, facilitar becas para cursos, etc. (De Lorenzo y Montero, 2003).

Las Administraciones y las instituciones sanitarias deben contemplar la realización adecuada de procesos de información como una medida de calidad de la Institución. Deberían, por tanto, desarrollarse indicadores de calidad adecuados, dirigidos a evaluar el esfuerzo de la institución y sus profesionales ante la implantación del consentimiento informado, y no a registrar sólo cuestiones puntuales y poco discriminativas, como puede ser analizar el número de documentos escritos informados por el Servicio, etc.

3.11.4.4 El derecho a no saber

Aquí también es conveniente hacer referencia al derecho a no saber por parte del paciente (artículo 9.1 de la Ley 41/2002). Esta situación supone una dejación voluntaria, por parte del enfermo, en manos del médico.

Este aspecto ya fue recogido en el artículo 10.2 del Convenio de Oviedo. Sin duda, los pacientes pueden tener sus propias razones para no desear conocer ciertos aspectos de su salud, lo cual, según algunos autores, no debe suponer un obstáculo para la validez de su consentimiento a una intervención determinada. El supuesto derecho a no ser informado ha sido objeto de numerosas discusiones por el hecho de que esta opción, aunque en principio pueda parecer en contrasentido, puede menoscabar la autonomía del sujeto (López Guzmán, 2004).

Sobre el derecho a no saber, también cabría plantear si el rechazo del paciente a ser informado por el médico tiene limitaciones. En la Ley 41/2002 sólo se indica que «cuando el paciente manifieste expresamente su deseo de no ser informado, se respetará su voluntad haciendo constar su renuncia documentalmente, sin perjuicio de la obtención de su consentimiento previo para la intervención».

3.11.4.5 El consentimiento informado

En la Ley 41/2002 se ofrece una gran atención al consentimiento informado. Ya se ha mencionado que este hecho ha sido una constante en los últimos años, no obstante, lo más relevante no es el protagonismo del consentimiento en la nueva disposición, sino el nuevo contexto en el que se le incluye. Hasta el momento de entrada en vigor de la nueva ley, ha habido un apogeo de los documentos escritos para la obtención del consentimiento informado: impresos estandarizados, no personalizados, que tenían como principal objetivo la defensa del facultativo ante posibles reclamaciones. El consentimiento informado es mucho más que un mero requisito legal, se trata en verdad de una obligación ética básica de todo profesional médico (no sólo el que actúa en un medio hospitalario), que responde a la necesidad de respetar la dignidad del paciente como persona (López Guzmán, 2004).

Estamos así ante una de las máximas manifestaciones del respeto a la autonomía del paciente, de tal forma, que como regla general, no puede llevarse a cabo ninguna actuación en el ámbito de la salud del paciente si él mismo no ha prestado su consentimiento.

Al cumplir la obligación de informar para obtener el consentimiento del paciente para el diagnóstico o tratamiento, el médico no se limita a cumplir una obligación legal y a protegerse contra una demanda de responsabilidad profesional. Por el contrario, estará realizando un acto clínico, elevando la calidad de la asistencia y propiciando que la relación médico-paciente se asiente en unas bases que conducirán a su mejor éxito, además, se supera la consideración tradicional de que lo que importa ante todo es el bienestar del paciente y se sustituye por el llamado principio de autonomía, es decir, el sometimiento voluntario a una actuación en el ámbito de la salud por su libre y soberana decisión, tratamiento además en el que deberá ser considerado como sujeto de derechos y deberes, que incluyen no sólo su salud, sino también el respeto a su dignidad humana e intimidad (De Lorenzo y Montero, 2003).

La línea propuesta por la Ley 41/2002 se aleja del frío cumplimiento de unos protocolos materiales para ahondar en el verdadero núcleo de la cuestión, la información y el diálogo. No obstante, cabría plantear si esta nueva forma de abordar el consentimiento informado está dirigida a una humanización del proceso en provecho del paciente, o si trata más bien de un intento de proteger a profesionales e instituciones de las continuas reclamaciones judiciales basadas en las omisiones producidas en los protocolos impresos (Palomares Bayo *et al.,* 2002).

3.11.4.6 **El consentimiento por representación**

En la Ley General de Sanidad se hacía referencia, al considerar la representación, al consentimiento dado por familiares y allegados sin establecer ningún orden prioritario a la intervención entre ellos. En la Ley 41/2002 desaparecen los allegados, esta mayor precisión redundará en la disminución de conflictos, ya que la de allegados era una figura dotada de un alto grado de indeterminación (López Guzmán, 2004).

3.11.4.7 Los menores de edad

En la Ley 41/2002 se encuentran, al menos dos posibles aspectos que pueden dar lugar a conflictos en la asistencia a menores maduros (de los 12 a los 16 años). El primero viene determinado por la eventualidad de que ante un tratamiento surja desacuerdo entre el hijo enfermo y sus padres, en este supuesto habría que tener en cuenta el criterio del Convenio de Oviedo y la Ley Orgánica 1/1996 de Protección al Menor, según los cuales la opinión del menor deberá ser tomada en consideración como un factor que será tanto más determinante en función de su edad y su grado de madurez, siempre que su parecer no vaya a causarle un daño (López Guzmán, 2004:36).

El segundo problema es la duda que se suscita cuando se presenta un menor sólo en la consulta, se ha señalado que puede ser beneficioso atenderle, ya que facilitará el clima de confianza que permitiría al facultativo desarrollar su actuación, pero este modo de proceder tiene en contra la vulneración de confianza creada si fuera necesario tener que informar a los padres (Abellán Sarlot, 2007).

A los menores emancipados y a los mayores de 16 años, la Ley 41/2002 no les reconoce capacidad para decidir sobre la interrupción del embarazo, la participación en ensayos clínicos y el sometimiento a técnicas de reproducción asistida, para ello se requieren 18 años, edad que la Constitución española y el Código Civil establecen con carácter general como mayoría de edad.

3.11.4.8 Necesidad terapéutica

Un aspecto relacionado con la información, contemplado por la Ley 41/2002, y que también hay que considerar que puede ser polémico, es el de la necesidad terapéutica o capacidad del facultativo de limitar la información para no perjudicar al paciente (artículo 5.4). Tradicionalmente, la necesidad terapéutica ha sido denominada privilegio terapéutico.

La necesidad terapéutica puede ser origen de debate en cuanto que limita la autonomía del paciente. Se justifica cuando se antepone la protección de la persona, que es substrato de los derechos o de su autonomía. Antepone la necesidad de cuidar y su invocación depende del sistema de referencia del profesional (López Guzmán, 2004).

Señala De Lorenzo y Montero (2003:44) que «el estado de necesidad terapéutica es un supuesto de información claramente perjudicial para la salud del paciente y, en este caso, es ineludible la valoración de los intereses en conflicto, para lo cual parece recomendable el asesoramiento del Comité Asistencial de Ética, siendo la intervención asesora del mismo especialmente recomendable cuando la situación descrita concurra con el deseo expresado por el paciente de conocer su verdadero estado de salud».

La necesidad terapéutica no debe ser confundida con el pronóstico fatal, puesto que éste último, tal y como ha señalado la doctrina, lejos de excluir el deber de informar constituye una manifestación importante de este deber y, en principio, es un derecho que corresponde a todo enfermo que quiera conocer su verdadero estado de salud. Otra cosa distinta es que este supuesto concurra con una renuncia del destinatario, expresa o tácita.

3.11.4.9 **El documento de voluntades anticipadas (instrucciones previas)**

He aquí otra de las cuestiones novedosas de la Ley 41/2002, la cual se halla regulada en el artículo 11 de la misma, bajo la denominación de instrucciones previas. La institución del documento de voluntades anticipadas, o instrucciones previas, trae su causa directa del Convenio de Oviedo, el cual se refiere a los deseos expresados anteriormente (De Lorenzo y Montero, 2003).

El concepto de las instrucciones previas lo ofrece el propio legislador en el artículo 11.1, según el cual: «Por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo. El otorgante del documento puede designar, además, un representante para que, llegado el caso, sirva como interlocutor suyo con el médico o el equipo sanitario para procurar el cumplimiento de las instrucciones previas».

A diferencia del consentimiento informado, en el que la regla general es que el mismo se presta verbalmente y sólo por escrito en los supuestos determinados por la ley, las instrucciones previas deben constar siempre por escrito, pudiendo ser revocadas libremente y en cualquier momento, dejando constancia de ello igualmente por escrito. Además, para procurar el cumplimiento de las instrucciones previas, se señala que el otorgante puede designar a un representante para que, llegado el caso, sirva como interlocutor con el médico o equipo sanitario (García Barrios, 2003).

En lo que se refiere a la forma de las instrucciones previas, ésta corresponde determinarla a las Comunidades Autónomas (cada Servicio de Salud regulará el procedimiento adecuado para que, llegado el caso, se garantice el cumplimiento de las instrucciones previas de cada persona, que deberán constar siempre por escrito), aunque la Ley 41/2002 también prevé la creación en el Ministerio de Sanidad y Consumo el Registro Nacional de Instrucciones Previas a fin de asegurar su eficacia en todo el territorio español (Palomares Bayo, 2002).

3.11.4.10 **La historia clínica**

La Ley 41/2002 también se refiere a la custodia de la historia clínica (artículo 17). Sin embargo, no ha definido la propiedad de este documento, mantiene la línea continuista de otras disposiciones precedentes.

El texto refleja que la historia clínica se redacta, en primer lugar en beneficio del paciente, no hay que olvidar que la historia clínica es el relato patobiográfico de una persona, por lo tanto afecta notoriamente a su intimidad. En cuanto al médico, la historia clínica puede ser su mejor amiga o peor enemiga cuando es procesado, por lo que no es extraña la reticencia de médicos y establecimientos sanitarios a cederle a los individuos que las protagonizan (López Guzmán, 2004).

Cabe resaltar que se tratará en extenso la historia clínica y la historia clínica electrónica en el próximo capítulo, haciendo en éste punto una breve mención.

3.11.4.11 **Responsabilidad compartida**

Por último hay que destacar que la ley hace partícipe a todo el equipo asistencial de la labor informativa, el artículo 4.3 de la Ley 41/2002, establece que «que los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle». Este reconocimiento es importante no sólo por el beneficio que una mayor información proporciona al paciente, sino también por lo que afecta a la asunción de responsabilidades por parte del equipo de atención sanitaria.

La prestación de una información adecuada al paciente, en atención a las circunstancias específicas, se configura, además de cómo un derecho de los pacientes o usuarios, cómo una obligación a cumplir por los profesionales sanitarios, y que, además, ha sido calificada por la jurisprudencia y por el legislador como un derecho fundamental (De Lorenzo y Montero, 2003).

Por tanto, la omisión o prestación defectuosa de la información y/o consentimiento se vienen configurando como una nueva fuente de responsabilidad profesional del médico, en particular, y del funcionamiento de los servicios sanitarios, en general (García Barrios, 2003).

CAPÍTULO IV
TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO SANITARIO DE BOLIVIA

4.1 EL RECURSO DE HÁBEAS DATA EN BOLIVIA

4.1.1 LA ANTIGUA CONSTITUCIÓN POLÍTICA DEL ESTADO DE 1967 Y SUS REFORMAS

El hábeas data, como una vía procesal instrumental de protección al derecho a la autodeterminación informática fue incorporado al sistema constitucional boliviano mediante la Ley 2631 de Reforma de la Constitución de 20 de febrero de 2004.

Como antecedente de la adopción del «hábeas data» como vía procesal instrumental de carácter tutelar, corresponde señalar lo que establecen Rivera Santibáñez *et al.,* (2005:124), que «en la Ley 2410 Declaratoria de Necesidad de Reforma se propuso ampliar el catálogo de los derechos fundamentales previsto en el artículo 7 de la Constitución, con la inclusión de otros derechos fundamentales, entre ellos, el derecho a la intimidad y privacidad, imagen, honra y reputación».

En concordancia con la propuesta de consagración del derecho a la vida privada en el catálogo de los derechos fundamentales, lo que supone el reconocimiento del derecho a la autodeterminación informática, en la Ley 2410 Declaratoria de Necesidad de Reforma, en el capítulo referido a las garantías constitucionales, se propuso instituir el Habeas Data como vía jurisdiccional expedita para que toda persona pueda acceder, objetar u obtener la eliminación o rectificación de sus datos personales registrados en bancos de datos o archivos públicos o privados. A este efecto la Ley 2410 se propuso modificar el texto del artículo 23 de la Constitución que consagraba la garantía de la prohibición de confiscación de bienes, para reemplazarlo con un nuevo texto que instituye el recurso de Hábeas Data.

Dada la coyuntura política y social que derivó de los acontecimientos de febrero y octubre de 2003, el Congreso Nacional, actuando como Constituyente derivado, conforme al procedimiento constitucional, ha procedido a la consideración, aprobación y sanción de la Ley 2631 de Reforma de la Constitución, en la que ha reformado 15 de los 35 artículos propuestos en la Ley 2410. Cabe advertir que entre los 15 artículos reformados no se ha incluido la modificación del artículo 7 de la CPE, de manera que no se ha incluido en el catálogo de los derechos fundamentales los derechos a la intimidad y privacidad, imagen, honra y reputación, por lo mismo que no se ha proclamado expresamente el derecho a la autodeterminación informática.

Empero, ello no impide que cualquier persona que considere lesionados esos derechos pueda solicitar la tutela correspondiente; ello en razón a que, si bien no están proclamados en el catálogo de derechos fundamentales de la Constitución, sí lo están en los instrumentos internacionales que ha suscrito o a los que se ha adherido el Estado boliviano y los ha ratificado mediante Ley de la República[25], como es el caso de la Declaración Universal de los Derechos Humanos (artículo 12), el Pacto Internacional de los Derechos Civiles y Políticos (artículo 17), y la Convención Americana sobre Derechos Humanos. Si bien no se ha proclamado expresamente el derecho a la «autodeterminación informática», si se ha instituido el Hábeas Data en el texto de la Constitución, como una garantía constitucional para la protección de aquel derecho.

El autor boliviano Rivera Santibáñez (2004:425) señala que «El hábeas data es un proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la autodeterminación informática, es una garantía constitucional que brinda a la persona una protección efectiva e idónea frente al manejo o uso ilegal e indebido de información o datos personales generados, registrados, almacenados en bancos de datos públicos o privados y distribuidos a través de los medios informáticos».

En efecto, el constituyente boliviano, al sancionar la Ley 2631 de fecha 20 de febrero de 2004, en el marco de la Ley 2410 de fecha 1.º

---

[25] Con la aprobación de la nueva Constitución Política del Estado en febrero de 2009 cambia la denominación de República de Bolivia por Estado Plurinacional de Bolivia.

de agosto de 2002, entre otras disposiciones, reforma el artículo 23 del texto de la Constitución en los términos siguientes:

I. «Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos, de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de Hábeas Data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.

II. Si el Tribunal o Juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado.

III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo.

IV. El recurso de Hábeas Data no procederá para levantar el secreto en materia de prensa.

V. El recurso de Hábeas Data se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el artículo 19 de esta Constitución».

4.1.2 CONCEPTO, NATURALEZA JURÍDICA Y ALCANCE DEL HÁBEAS DATA

Según la doctrina, el Hábeas Data es una garantía constitucional de carácter procesal para la protección de los datos personales, aquellos que forman parte del núcleo esencial del derecho a la privacidad o la intimidad de una persona, frente a la obtención, almacenamiento y distribución ilegal, indebida o inadecuada por entidades u organizaciones públicas o privadas. Esta garantía constitucional otorga a toda persona sea natural o jurídica, la potestad y facultad, el derecho de acudir a la jurisdicción constitucional para demandar a los bancos de datos y archivos de entidades públicas y privadas con el fin de que le permitan el conocimiento, la actualización, la rectificación o supre-

sión de las informaciones o datos referidos a ella, que hubiesen obtenido, almacenado o distribuido (Rivera Santibáñez *et al.*, 2005).

El autor boliviano Arce Jofré (2003:45) establece que «La acción de Hábeas Data se define como la garantía constitucional que asiste a toda persona (identificada o identificable) a solicitar judicialmente la exhibición de los registros (públicos o privados) en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud, a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación. Tiende a proteger a la persona contra calificaciones sospechosas incluidas en registros que pueden llegar a perjudicar de cualquier modo».

La posición dominante de la doctrina en países de la región andina y de la cuenca del atlántico, en la última década reposa en Alicia Pierini, Valentín Lorences y María Inés Tornabene (1999:17) citados por Perales Gareca (2004:21), quienes asumen que «la acción de Hábeas Data es una modalidad de amparo que permite a toda persona interesada acceder al conocimiento de los datos que consten en registros de bancos de datos públicos o privados destinados a proveer informes, y a exigir su supresión, rectificación, confidencialidad o actualización, en caso de falsedad o discriminación; información que debe referirse a cuestiones relacionadas con la intimidad o privacidad, no pudiendo utilizarse por terceros sin derecho a hacerlo».

El Hábeas Data es una garantía constitucional que sin desconocer el derecho a la información, al trabajo y el comercio de las entidades públicas o privadas mantienen centrales de información o bancos de datos, reivindica el derecho que tiene toda persona a verificar qué información o datos fueron obtenidos, almacenados sobre ella, cuáles de ellos se difunden y con qué objeto, de manera que se corrijan o aclaren la información o datos inexactos, impedir que se difundan y, en su caso se eliminen si se tratan de datos o informaciones sensibles que lesionan su derecho a la vida privada o íntima en su núcleo esencial referida a la honra, buena imagen o el buen nombre.

Como una vía procesal de carácter instrumental de tutela al derecho a la autodeterminación informática, el hábeas data se activa en aquellos casos en los que la persona afectada reclama ante la entidad pública o privada encargada del banco de datos, la entrega de la información o datos personales obtenidos y almacenados, en su caso la actualización, rectificación o supresión de aquella información o da-

tos falsos o incorrectos, y no obtiene una respuesta positiva, es decir, que la entidad pública o privada no asume inmediatamente la acción solicitada.

Según la doctrina y la legislación comparada, la protección que brinda el Hábeas Data abarca los siguientes ámbitos:

— *Acceso y control de la información personal:* El hábeas data se presenta inequívocamente como una acción para recabar y obtener información sobre datos personales que conciernen al titular (sea persona natural o jurídica), que obren en registros informáticos o mecánicos de la Administración Pública o sociedades privadas; petición que en ejercicio de su derecho de ejercer el control y sigilo en resguardo de su dignidad y desarrollo de su personalidad, los responsables de dicha información están obligados a proporcionar, con la excepcionalidad de la ley para supuestos en que los límites del derecho sean dignos de mantenerse justificados, previa valoración judicial, lo que parece ser en estos casos una solución equitativa.

— El derecho de acceso no ha de implicar necesariamente que el interesado, ante supuestas sospechas de afectación en la recogida y tratamiento de datos, tenga que accionar demandando la actuación de la administración o de los responsables de los ficheros; sino que ésta tiene la obligación de prestar información completa y verdadera a los interesados tan pronto posean en su poder información y se prevea el destino que pretenden darle. Con la exigencia cumplida que se apunta, se podrían evitar problemas singulares. El acceso podrá efectuarse por vía administrativa, o bien por vía judicial.

— *Actualización de datos personales:* El derecho a la actualización permite que la persona informada del conocimiento de los datos que le conciernen (o una tercera persona a su nombre con poder especial) y que haya constatado que éstos no guardan relación con el objeto de su versión original, por haberse generado efectos subsecuentes y cualitativos de orden relevante para su personalidad, tiene la facultad de exigir que los mismos sean puestos al día por los responsables o encargados de los ficheros, con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona. Así por ejem-

plo: si aparece como condenado en los registros, que conste su sobreseimiento o absolución y, si se ha cumplido con la condena impuesta, que se suprima su registro judicial y penitenciario.

— *Rectificación de datos personales:* El derecho de rectificación o corrección supone que el interesado, que con antelación tuvo acceso a la fuente de datos registrados, al verificar que son inexactos o erróneos, requiere al órgano pertinente que proceda a corregir la información registrada y, en caso de haberse producido la transmisión, informar de esta medida a los destinatarios de los datos cedidos o transferidos, a efecto de insertar la rectificación.

— *Confidencialidad:* Es el supuesto de que el interesado, habiendo consentido voluntariamente proporcionar la información requerida legalmente por la Administración Pública, exige al poder público que dicha información permanezca reservada o secreta para terceros, y en caso de ser susceptible de transmisión a otro ente de la misma naturaleza y con fines similares o diferentes al de su acopio original, corresponderá informar al interesado de esta decisión, a los efectos de preservar sus derechos fundamentales. Encaja en esta categoría del derecho el secreto fiscal o secreto bancario, el secreto médico, el secreto del profesional abogado y la Declaración Jurada de Bienes ante la Contraloría General del Estado.

— *Cancelación de datos personales*[26]*:* En esta gama de derechos que tutela el Hábeas Data y que proceden de una misma ma-

---

[26] La Sentencia Constitucional 0851/2013-L de fecha 14 de agosto de 2013 establece *FUNDAMENTOS JURÍDICOS DEL FALLO: La accionante se refiere a que se encuentra registrada en la base de datos de la FELCC, una denuncia en su contra por los delitos de lesiones graves y leves, además de amenazas, misma que dataría de hace más de diez años, la que jamás se llegó a investigar ni procesar, por lo que habiendo solicitado su cancelación las autoridades ahora demandadas, habrían negado anular ese antecedente, por lo que al mantener subsistentes esos datos se afectaría sus derechos a la dignidad, al respeto y a la privacidad, impidiéndole acceder a un certificado negativo de antecedentes penales. Al respecto, en revisión, corresponde analizar, si tales argumentos son evidentes a fin de conceder o denegar la tutela impetrada… POR TANTO: El Tribunal Constitucional Plurinacional, en su Sala Liquidadora Transitoria, en virtud de lo previsto en el art. 20.II de la Ley 212 de 23 de diciembre de 2011; en revisión, resuelve: 1.° CONFIRMAR en parte la Resolución 01/2011 de 17 de noviembre, cursante a fs. 30*

triz, se habilita al interesado en uso de un haz de poderes, para solicitar al órgano público o privado la cancelación de datos referidos al origen racial, la salud, las creencias religiosas, la filiación política o sindical y tendencias sexuales, por estimarse que las dimensiones internas y externas de estos derechos al ser inherentes a la dignidad de la persona, deben estar dirigidos en todo caso al ejercicio libre y consiguiente desarrollo de la personalidad del individuo que vive en un Estado de derecho de valores superiores. De esto se desprende que los supuestos que motivan la petición de cancelación integran los datos concebidos como *«información sensible»*, pero bien pudiera ser que otros, irrelevantes en su recogida inicial, alcancen con el tratamiento posterior relevancia y revista mayor interés su preservación. Esto equivale a sostener que en la actualidad todos los datos de una persona son importantes y de inusitado interés (Gareca Perales, 2004 y Rivera Santibáñez *et al.* 2005).

4.1.3 DERECHOS QUE PROTEGE EL HÁBEAS DATA

Según lo dispuesto por la norma objeto de la investigación, el Hábeas Data brinda tutela efectiva a los derechos fundamentales a la intimidad y privacidad personal y familiar, a la imagen, honra y reputación de las personas, referidas al ámbito de manejo de los datos o informaciones obtenidos y almacenados en los bancos de datos públicos o privados; lo que en resumen, supone una protección al derecho a la autodeterminación informática, permitiéndole el acceso a los datos o informaciones obtenidas, almacenadas y distribuidas por los bancos de datos públicos o privados, para lograr su conservación, rectificación o supresión.

---

a 33, pronunciada por la Sala Civil Segunda de la Corte Superior del Distrito Judicial -ahora Tribunal Departamental de Justicia- de Tarija; y, en consecuencia: CONCEDER la tutela solicitada, sólo con relación al Director Departamental de la FELCC de Tarija; y, DENEGAR la misma con relación al Fiscal de Distrito de ese mismo departamento. 2° Disponer la cancelación del acta de denuncia signado como caso PTJ100225 de 30 de mayo de 2001, de los archivos de la FELCC de Tarija.

El derecho a la autodeterminación informativa y libertad, entendida esta en cuanto posición jurídica subjetiva correspondiente al status de hábeas data, que pretende satisfacer la necesidad sentida por las personas en la sociedad informatizada de la vida social, de preservar su identidad, controlando cómo y para qué fines se recaban sus datos personales, con qué propósitos se practican interconexiones y transferencias, qué seguridad se otorga a la cualidad y pertinencia de los mismos y que éstos en el marco de la confidencialidad serán herméticamente guardados por el tiempo necesario que evite generar amenazas o peligros, no solo a los derechos que conforman el conjunto de las pautas privadas del entorno personal, familiar, profesional en su perspectiva patrimonial, tributaria, financiera y comercial, sino en todos aquellos datos sensibles de carácter personal que revelan el origen racial, las opiniones políticas, las convicciones religiosas, los estados de salud, la vida sexual y las filiaciones asociativas o sindicales (Gareca Perales, 2005 y Sentencia Tribunal Constitucional 292/2000[27]).

En definitiva el Hábeas Data en el sistema constitucional boliviano, tiene por fines proteger el derecho a la autodeterminación informática de la persona, garantizando el ejercicio de los siguientes derechos:

— *De acceso a los datos o información referidos a su persona*, que hubiesen obtenido y almacenado los bancos de datos públicos o privados, para conocer qué informaciones se consignan sobre su persona, con qué fundamentos; asimismo, conocer los fines y objetivos de la obtención y almacenamiento, es decir, qué uso le darán a esa información, de manera que su acceso a la base de datos del banco informatizado de la Administración Pública o privada, le brinde la oportunidad de obtener información y comprobar la finalidad que se imprime a su tratamiento, desde la fecha en que fue almacenada sea con autorización del titular de los datos, o si fue recogida de repertorios públicos como guías telefónicas, direcciones de Colegios de profesionales, etc.

---

[27] Sentencia del Tribunal Constitucional español 292/2000, de 30 de noviembre, interpuesto por el Defensor del Pueblo contra los artículos 21.1 y 24.1 de la ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD).

— *De rectificación*[28] *o corrección de la información obtenida y almacenada*[29], si la misma contiene datos personales falsos o

---

[28] Sentencia Constitucional 0332/2015 S1 de fecha 6 de abril de 2015 establece en «III. FUNDAMENTOS JURÍDICOS DEL FALLO: *La accionante denunció que el Juez demandado vulneró sus derechos a la dignidad, a la imagen honra y reputación, al haber insertado en la Resolución de 5 de marzo de 2014, la frase: "luego de acompañarme me asaltó" (sic), agraviando su dignidad y honra, lesiones que a pesar de haber sido objeto de solicitud de explicación, enmienda, apelación y reposición fueron mantenidas en desmedro de su dignidad y su derecho al debido proceso. Por lo que, corresponde analizar en revisión si los actos denunciados son evidentes a objeto de conceder o denegar la tutela solicitada*». III.2 Análisis del caso concreto…» *Por lo que, corresponde analizar en revisión si los actos denunciados son evidentes a objeto de conceder o denegar la tutela solicitada. En este sentido resulta claro que la supuesta expresión indignante, fue insertada por el Juez ahora demandado en la Resolución de 5 de marzo de 2014, siendo ratificada posteriormente en todas sus partes mediante Auto de Vista 143/14, fallos que no se constituyen en bancos de datos de registro de información, sino que corresponden al análisis de elementos de hecho y derecho aportados en el proceso de investigación; por lo que en el marco del Fundamento Jurídico III.1 de la presente Sentencia Constitucional Plurinacional, es importante considerar que la acción de protección de privacidad se constituye en una garantía para conocer, verificar y corregir información contenida en los archivos de entidades, no así dentro de expedientes o cuadernos de investigación; de esta manera a través de la reiterada jurisprudencia constitucional se ha establecido como requisitos indispensables para su procedencia que éstos sean públicos o privados, físicos, electrónicos, magnéticos u informáticos, tengan como finalidad proveer informes y su necesaria vinculación de los derechos protegidos por esta acción; presupuestos que en el caso en análisis no se cumplen ante la inexistencia de una base de datos o registros; por lo que no es posible examinar los hechos denunciados, dada su naturaleza jurídica y alcances, aspectos que al tratarse de defectos u observaciones dentro de un proceso judicial pudieron haber sido cuestionados mediante la acción de amparo constitucional por la amplitud de su ámbito de tutela y resguardo de derechos*».

[29] Sentencia Constitucional Plurinacional 0426/2015-S3 de fecha 20 de abril de 2015. III. FUNDAMENTOS JURÍDICOS DEL FALLO: «*El accionante denuncia la vulneración de sus derechos a la privacidad e intimidad, honra, honor, propia imagen y dignidad, a la autodeterminación informativa y al trabajo, alegando que el Banco de Crédito de Bolivia S.A., le registró un «código de desvinculación laboral» o «código de retiro» injusto e ilegal que luego fue informado a la ASFI, sin tener en cuenta que al haber renunciado le correspondía el código 110 (referido «renuncia, finalización de contrato,*

errados, cuya difusión podría causar graves daños y perjuicios a la persona registrada en el banco de datos, como ejemplo, corregir una situación deficitaria de insolvencia bancaria por error en la persona obligada o se registre una condena penal en los datos personales cuando esa persona jamás fue sometida a proceso penal alguno; por lo mismo jamás fue condenado a sufrir pena alguna.

---

retiro por jubilación o fallecimiento») y no así el código 103 (referido a «retiro forzoso por contravenciones graves a normas internas o disposiciones legales, por imprudencia o negligencia culposa, con daño económico y sin fórmula de solución voluntaria»), por cuanto respecto de este último supuesto, nunca fue sometido a un proceso previo donde se compruebe su supuesta falta; añadiendo que dicha codificación injusta e ilegal no le permite trabajar en otra entidad de intermediación financiera. Razón por la cual, peticiona se rectifiquen sus datos, recodificándose su desvinculación laboral de la asignación del código 103 por el código 110. En consecuencia corresponde determinar en revisión, si se debe conceder o denegar la tutela solicitada». POR TANTO: «El Tribunal Constitucional Plurinacional, en su Sala Tercera; en virtud de la autoridad que le confiere la Constitución Política del Estado y el art. 12.7 de la Ley del Tribunal Constitucional Plurinacional; en revisión, resuelve:…2.º Disponer se proceda a la recodificación del registro del dato, esto es, respecto a la causa de desvinculación del accionante la que se produjo, por renuncia a la entidad supervisada del Banco de Crédito de Bolivia S.A., sea conforme al procedimiento previsto en el Reglamento para el Registro de Directores, Síndicos, Fiscalizadores Internos, Inspectores de Vigilancia, Ejecutivos y demás funcionarios».

— *De obtener la eliminación*[30] *o exclusión de la llamada información sensible*[31], relacionada al ámbito de su intimidad o la de su familia, es decir, aquellos datos mediante los cuales pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como el origen racial, las opiniones políticas, las convicciones religiosas, los estados de salud, la vida sexual y las filiaciones asociativas o sindicales. La elimina-

---

30 Sentencia Constitucional 0189/2010-R de fecha 24 de mayo de 2010, III FUNDAMENTOS JURÍDICOS DEL FALLO: «*…es imperante determinar con claridad el objeto y la causa del presente recurso de hábeas data, actualmente denominado acción de protección de privacidad, razón por la cual, se tiene que en la especie, el objeto de la tutela pedida es la eliminación de datos supuestamente falsos cursantes en los archivos públicos de la INTERPOL y la Dirección Nacional de Identificación, para la protección de los derechos de los recurrentes a la dignidad, a la vida privada, a la honra, al honor, a la reputación y a la personalidad. Asimismo, se establece que la causa de la petición de tutela es la supuesta existencia de datos denunciados como falsos que afectan los derechos antes descritos de los recurrentes, ahora accionantes. Por lo expuesto y una vez identificado el objeto y la causa del presente recurso, corresponde verificar si los derechos denunciados como vulnerados merecen la protección de tutela constitucional en el marco de los alcances de los arts. 23 de la CPE abrogada y 130 de la Constitución Política del Estado vigente (CPE)*».

31 Sentencia Constitucional 1738/2010-R de fecha 25 de octubre de 2010, III. FUNDAMENTOS JURÍDICOS DEL FALLO: «*La recurrente ahora accionante denuncian la vulneración de los derechos de su representada a la privacidad, dignidad, intimidad, decoro, honor y a la «seguridad jurídica», aduciendo que su representada menor de edad V.G.Z., tuvo una relación íntima con su ex enamorado ahora demandado, quien mediante un aparato celular procedió a filmar parte de la relación sexual, la cual posteriormente circuló en la página web Bolivia.com, así como en los aparatos celulares de los alumnos y docentes de la universidad donde estudiaba, por lo que ante este daño moral, psicológico, espiritual, emocional que va contra la dignidad, personalidad, decoro y fundamentalmente la intimidad de su representada, se vio obligada a impedir que continúe asistiendo a la universidad, por la serie de comentarios y discriminaciones de la que fue objeto no sólo su representada sino toda su familia, máxime si su actividad laboral es de maestra normalista del nivel secundario. Consiguientemente, en revisión de la Resolución del Tribunal de garantías corresponde determinar si se debe otorgar o no la tutela impetrada*».

ción de los datos[32] por causarle graves daños y perjuicios no es otra cosa que su cancelación o destrucción del programa en

---

[32] Sentencia Constitucional 0192/2015 S2 de fecha 25 de febrero de 2015 establece III. FUNDAMENTOS JURÍDICOS DEL FALLO: *«El accionante denuncia la vulneración de sus derechos a la propia imagen, honra y reputación, por cuanto la FELCN de Beni, de forma ilegal, sin que exista proceso abierto o sentencia ejecutoriada inscribió un antecedente policial en su contra y al acudir a través de la representación de su hermana ante la Fiscalía Departamental de Beni y a dependencias de la FELCN, solicitando se borre el mismo, no se procedió conforme a lo incoado. En consecuencia, corresponde analizar, en revisión, si los argumentos son evidentes a fin de conceder o denegar la tutela solicitada»*. III.3. La cancelación de antecedentes policiales en los casos en que no se haya iniciado proceso alguno ni investigación contra la persona que lo solicita, no requiere orden judicial: *«Bajo esa óptica, tomando como parámetro el asunto que ahora se dilucida, se concluye que no es exigible la presentación de orden judicial expresa ante la FELCN, para la cancelación de antecedentes policiales, cuando no se inició proceso ni investigación alguna contra la persona que lo solicita, porque ello implicaría establecer un requisito formal que no tiene razón de ser, por el mismo hecho de que no se le abrió causa penal; pudiendo consecuentemente la misma dirigir directamente su pretensión ante la institución referida para la solicitud de cancelación de antecedentes policiales y en caso de contar con su negativa, interponer la acción de protección de privacidad, demostrando la no existencia de apertura de proceso penal ni investigativo en su contra. Bajo esa óptica, tomando como parámetro el asunto que ahora se dilucida, se concluye que no es exigible la presentación de orden judicial expresa ante la FELCN, para la cancelación de antecedentes policiales, cuando no se inició proceso ni investigación alguna contra la persona que lo solicita, porque ello implicaría establecer un requisito formal que no tiene razón de ser, por el mismo hecho de que no se le abrió causa penal; pudiendo consecuentemente la misma dirigir directamente su pretensión ante la institución referida para la solicitud de cancelación de antecedentes policiales y en caso de contar con su negativa, interponer la acción de protección de privacidad, demostrando la no existencia de apertura de proceso penal ni investigativo en su contra»*. POR TANTO: *«El Tribunal Constitucional Plurinacional, en su Sala Segunda, en virtud de la autoridad que le confiere la Constitución Política del Estado, de conformidad con el art. 44.2 del Código Procesal Constitucional, en revisión, resuelve: REVOCAR en parte la Resolución 22/2014 de 5 de agosto, cursante de fs. 65 a 67 vta., pronunciada por la Sala del Trabajo y Seguridad Social del Tribunal Departamental de Justicia de Beni; y, en consecuencia: 1° CONCEDER la tutela solicitada, con relación al Director Departamental de la FELCN de Beni, ordenando a dicha autoridad la eliminación del antecedente policial del accionante cuyo*

que fueron utilizados, por citar que se hagan conocer en un sistema de red, que la persona está siendo juzgada por delitos de lesa humanidad, cuando en realidad se trata de un homónimo, o bien que se muestre en la pantalla imágenes de su persona, sin que ella hubiere dado su consentimiento y todo tratamiento con datos sensibles.

Cabe advertir que, el constituyente ha incurrido en una lamentable omisión que arrastra desde la propuesta formulada en la Ley 2410, que debió ser subsanada en la Ley de Reforma de la Constitución, pues la norma prevista por el artículo 23 de la Ley fundamental no incluye en los alcances del Hábeas Data la protección de los siguientes derechos:

— *De confidencialidad de los datos personales*, es decir, que se guarde reserva absoluta de aquellos que le confió el titular del derecho a la autoridad recurrida. Resulta un ámbito importante en el cual se lesiona el derecho a la vida privada o la intimidad, cuando las entidades públicas o privadas que mantienen los bancos de datos o archivos transmiten de manera indebida, incorrecta y no autorizada los datos que fuesen suministrados por una persona; por ejemplo, no ceder o transferir datos que tienen relación con el hijo adoptivo a quien la sociedad considera como legítimo, habido dentro de matrimonio, o que la Contraloría General del Estado ceda los datos personales de la Declaración Jurada dispuesta por ley, recabados anualmente con fines tributarios a los ciudadanos, para ser utilizados por terceros con fines distintos de publicidad subjetiva, por la que se pone en duda la legalidad del patrimonio de la persona y su honestidad, a través de juicios paralelos.

— *De actualización de sus datos personales registrada o archivada en los bancos de datos públicos o privados*, que no es más que poner al día la información, que por descuido en el control del ente público o privado sigue manteniendo una situación pasada o se hubiese omitido registrar algún dato personal, por ejemplo, que el deudor del crédito bancario siga figurando en los programas de débito, siendo que canceló totalmente la deu-

---

registro se cuestionó, siempre y cuando producto de la determinación del Tribunal de garantías ello no se hubiere realizado…».

da contraída, lo que le ocasiona perjuicios en otras entidades crediticias donde tiene solicitado un nuevo préstamo (Rivera Santibáñez *et al.*, 2005).

La segunda omisión es subsanable por la vía interpretativa, en cambio la solución a la primera omisión es más complicada. Corresponderá al Tribunal Constitucional Plurinacional[33] hacer una interpretación constitucional de la norma prevista por el artículo 130.I aplicando los principios de la concordancia práctica y la eficacia o efectividad, para subsanar las omisiones referidas.

4.1.4 LÍMITES DEL HÁBEAS DATA

Siguiendo la doctrina de Derecho Procesal Constitucional, corresponde advertir que el Hábeas Data tiene un límite en cuanto a los alcances del Hábeas Data que se establece en el ejercicio de la libertad o derecho de información y libertad de expresión; pues no se activa contra la difusión de información a través de los medios masivos de comunicación social, toda vez que esta acción tutelar no es la vía adecuada para viabilizar el derecho de réplica por parte de un medio de prensa con relación a una información difundida que la persona considere inexacta o que agravia su derecho al honor, la honra o la buena imagen o lesione su vida privada o íntima.

Señala Rivera Santibáñez *et al.* (2005:123) que «no se descarta un mal uso que pueda hacerse de esta vía procesal, como sucedió en Perú donde se empleó como mecanismo de rectificación de la información, lo cual desnaturaliza la finalidad de esta vía procesal de protección del derecho a la autodeterminación informática».

El Hábeas Data no es un medio para ejercer control sobre los medios de comunicación social y el ejercicio de la libertad de expresión

---

[33] El Capítulo Sexto Tribunal Constitucional Plurinacional, artículo 196 de la Constitución Política del Estado establece: «*I. El Tribunal Constitucional Plurinacional vela por la supremacía de la Constitución, ejerce el control de constitucionalidad y precautela el respeto y la vigencia de los derechos y garantías constitucionales. II. En su función interpretativa, el Tribunal Constitucional Plurinacional aplicará como criterio de interpretación, con preferencia, la voluntad del constituyente, de acuerdo con su documentos, actas y resoluciones, así como el tenor literal del texto*».

e información, no es un mecanismo para establecer censura previa ni correctiva al ejercicio de estos derechos. Por ello, la norma prevista por el artículo 130.II de la Constitución dispone que la Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa, lo cual constituye una garantía para evitar cualquier pretensión de utilizar esta acción tutelar para levantar el secreto de la fuente en materia de ejercicio de la libertad de información y libertad de expresión (Rivera Santibáñez, 2010).

4.1.5 JURISPRUDENCIA DEL RECURSO DE HÁBEAS DATA Y ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

El Tribunal Constitucional, órgano que por su género único e indiscutible garante de la Constitución, los derechos fundamentales y garantías en ella contenida, perfilará en cada caso que motive la acción procesal instrumental, las subreglas encaminadas a sentar las líneas integradoras en la configuración institucional del Hábeas Data, a efecto de convertirlo en un verdadero instrumento de garantía real, inmediata y eficaz, ante el riesgo ilícito y discriminatorio que genera la informática en el procesamiento de datos personales.

El Tribunal Constitucional en su primigenia Sentencia Constitucional 0965/2004 de fecha 23 de junio de 2004, dentro del recurso de Hábeas Data interpuesto por J.C.V., contra G.T.O., Gerente General del periódico «La Razón» y E.O.A.B., alegó la vulneración de los derechos al honor, a la dignidad, a la imagen, a la intimidad y a la privacidad, por la publicación como deudor moroso que se hizo de su persona, a solicitud del recurrido en el medio de prensa escrito.

La Sentencia Constitucional 0965/2004 de fecha 23 de junio de 2004 y otras sentencias constitucionales, crean las subreglas en relación al derecho a la autodeterminación informática, reconoce la protección de la persona jurídica, la actualización de los datos, la confidencialidad y los datos sensibles, entre otros.

La jurisprudencia sentada hasta la fecha sobre el Recurso de Hábeas Data, hoy Acción de Protección de Privacidad, ha sido declarada improcedente por el Juez o Tribunal competente, debido a que no ha

fallado en el fondo de la cuestión, sino en la forma por la falta del agotamiento de la vía administrativa o judicial correspondiente.

4.1.5.1 El derecho a la autodeterminación informática

La Jurisprudencia del Tribunal Constitucional establece en la Sentencia Constitucional 965/2004-R que «… el hábeas data es una garantía constitucional que tiene por objetivo contrarrestar los peligros que conlleva el desarrollo de la informática en lo referido a la distribución o difusión ilimitada de información sobre los datos de la persona; tiene por finalidad principal proteger el derecho a la autodeterminación informática, preservando la información sobre los datos personales ante su utilización incontrolada, indebida e ilegal, impidiendo que terceras personas usen datos falsos, erróneos o reservados que podrían causar graves daños y perjuicios a la persona…».

En la misma Sentencia Constitucional señala «En cuanto a los límites del Hábeas Data, es importante remarcar que, como vía procesal instrumental, protege a la persona en su derecho a la autodeterminación informática, activándose contra el poder informático. De manera que cabe advertir que existe un límite en cuanto a los alcances del hábeas data que se establece en el ejercicio de la libertad o derecho de información y libertad de expresión».

La Sentencia Constitucional 0030/2006-R de 11 de enero de 2006, establece el ámbito de protección de esta acción tutelar en Bolivia en los siguientes términos: «El hábeas data como una vía procesal instrumental de protección al *derecho a la autodeterminación informativa*, referido a los derechos fundamentales a la intimidad y la privacidad de la persona, fue incorporado al sistema constitucional boliviano mediante la Ley 2631 de Reforma de la Constitución de 20 de febrero de 2004».

En el sistema constitucional boliviano, el hábeas data es una vía procesal instrumental para protección del derecho a la «autodeterminación informativa», precautelando que la persona pueda acceder al conocimiento de los datos o informaciones, referidos a su vida privada o íntima, así como la de su familia, obtenidos y almacenados en los bancos de datos públicos o privados, con la finalidad de conocer qué datos se han obtenido y almacenado; es decir, cuánta informa-

ción, con qué finalidad y a quienes se distribuyó, se distribuye o distribuirá la misma.

La Sentencia Constitucional 0189/2010 – R de 24 de mayo de 2010 establece: «… En ese orden, cabe precisar que la teoría general de los Derechos Humanos, en su clasificación, reconoce dos categorías concretas de derechos a saber: En primer orden se encuentran los derechos fundantes, como ser el Derecho a la vida o la libertad de tránsito entre otros y en segundo lugar, se tienen los derechos fundamentales derivados, entre los cuales inequívocamente se encuentra el llamado derecho de «autotutela informativa».

En efecto, el derecho a la «autotutela informativa» deriva directamente del derecho fundamental a la dignidad, a partir del cual, toda persona tiene el derecho de acceder, conocer, pedir rectificación, modificación o eliminación de datos que le conciernan y que le afecten o puedan atentar a sus derechos a la intimidad, privacidad personal o familiar, a la imagen, honra y reputación; generando para el administrador de estos datos contenidos cursantes en archivos públicos o privados, la obligación de garantizar este derecho fundamental, siempre y cuando no exista una norma expresa que prohíba dicho acceso, conocimiento, modificación o eliminación, ya sea por afectación a terceros, a la seguridad colectiva o por encontrarse sometidos al secreto o reserva.

En ese contexto, se establece que la génesis constitucional del derecho a la «autotutela informativa» encuentra cauce jurídico en el bloque de constitucionalidad boliviano, específicamente en el art. 21.6 de la Constitución vigente; asimismo, su contenido se encuentra sustentado por los artículos 13 del Pacto de San José de Costa Rica, 19 de la Declaración Universal de los Derechos Humanos y 19.2 del Pacto Internacional de Derechos Civiles, adoptado por la Asamblea General de la Organización de Naciones Unidas; además es importante señalar también que este derecho encuentra fundamento en la Resolución 1932 de la Organización de Estados Americanos, adoptada en su sesión plenaria de 10 de junio de 2003, que por su naturaleza en el marco del artículo 410[34] de la CPE, forma parte del Bloque de Cons-

---

[34] Artículo 410 de la Constitución Política del Estado, establece: «La Constitución es la norma suprema del ordenamiento jurídico boliviano y goza de primacía frente a cualquier otra disposición normativa. El bloque de consti-

titucionalidad y que garantiza el libre acceso a la información de todo Estado Democrático.

De lo expresado precedentemente, a partir del marco normativo descrito, se colige que el derecho a la «autotutela informativa», al margen de ser un derecho derivado, es también un derecho sustantivo, por tanto, en un Estado Social y Democrático de Derecho debe ser defendido por medios jurídicos idóneos, que logren su respeto efectivo».

4.1.5.2 **La persona física o jurídica**

La Jurisprudencia del Tribunal Constitucional establece en la Sentencia Constitucional 965/2004-R que «La legitimación activa del hábeas data recae en la persona natural o jurídica –aunque el precepto constitucional no lo determina de esa manera en forma expresa, se entiende que dentro de la protección de este recurso se puede y debe abarcar tanto a las personas físicas como a las jurídicas, de quienes también se pueden registrar datos e informaciones– respecto de la cual la entidad pública o privada haya obtenido y tenga registrados datos e informaciones que le interesen a aquella conocer, aclarar, rectificar, modificar, o eliminar, y que no haya tenido respuesta favorable por la citada entidad para lograr esos extremos».

El artículo 56 del Código Civil boliviano establece «que las personas colectivas deben adoptar, a tiempo de constituirse, un nombre al cual es aplicable lo dispuesto por el artículo 12». El artículo 12 señala: «La persona a quien se discuta el derecho al nombre que lleva o sufra algún perjuicio por el uso indebido de que ese nombre haga otra persona, puede pedir judicialmente el reconocimiento de su derecho o

---

tucionalidad está integrado por los Tratados y Convenios internacionales en materia de Derechos Humanos y las normas de Derecho Comunitario, ratificados por el país. La aplicación de las normas jurídicas se regirá por la siguiente jerarquía, de acuerdo a las competencias de las entidades territoriales: 1) Constitución Política del Estado; 2) Los tratados internacionales; 3) Las leyes nacionales, los estatutos autonómicos, las cartas orgánicas y el resto de legislación departamental, municipal e indígena; 4) Los decretos, reglamentos y demás resoluciones emanadas de los órganos ejecutivos correspondientes».

la cesación del uso lesivo. El juez puede ordenar que la sentencia se publique por la prensa».

La nueva Constitución Política del Estado vigente cambia el *nomen juris* del hábeas data a Acción de Protección de Privacidad, pero no así su esencia tutelar, empero contempla algunos cambios específicos en cuanto a su redacción, en especial el art. 130.I, en el que se refiere a los casos de legitimación activa que si bien es muy similar al texto del art. 23.I de la abrogada CPE, tiene una diferencia notoria cuando afirma: «Toda persona individual o *colectiva* que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad».

Se observa, en primer lugar, que se añaden a las personas colectivas como posibles legitimados activos, o futuros accionantes, concibiendo que las personas colectivas también tienen acceso a los derechos reconocidos por el art. 21.2 de la CPE, los cuales son: derecho a la intimidad, a la privacidad, honra, propia imagen y dignidad. Se entiende que el texto del artículo 130.I al reconocer como posibles accionantes a personas colectivas, se refiere a aquellas de orden público como privado, pero con algunas diferencias en cuanto a los derechos tutelados para estas, es decir, que las personas colectivas no podrán aducir la vulneración de su derecho a la intimidad personal y familiar, que son derechos fundamentales de índole personal, pero sí podrían denunciar la vulneración de sus derechos a la imagen y reputación.

Corresponde aclarar que si bien el derecho a la imagen, a la honra y a la reputación, parecieran estar dentro del mismo grupo de derechos tutelados por la Acción de Protección de Privacidad, en el caso de las persona colectivas, que es el objeto del presente análisis, como se indica líneas supra, sólo podrían denunciar la vulneración de los derechos a la imagen y la reputación, pero no así de la honra, debido a que el derecho a la honra es de índole estrictamente personal, es decir, entra dentro de la esfera de la personalidad y es concebido doctrinalmente como la pretensión de respeto que corresponde a cada

persona como reconocimiento de su dignidad frente a la sociedad (Sentencia Constitucional 1978/2011-R de fecha 7 de diciembre de 2011).

4.1.5.3 La actualización de los datos personales

La Jurisprudencia del Tribunal Constitucional a través de la Sentencia Constitucional 0965/2004-R de 23 de junio de 2004 establece sobre la actualización: «b) Derecho a la actualización de la información o los datos personales registrados en el banco de datos, añadiendo los datos omitidos o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona».

4.1.5.4 La confidencialidad

La Jurisprudencia del Tribunal Constitucional a través de la SC 0965/2004-R de 23 de junio de 2004, establece sobre la confidencialidad: «d) Derecho a la confidencialidad de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona».

4.1.5.5 Datos sensibles

La Jurisprudencia del Tribunal Constitucional a través de la Sentencia Constitucional 0965/2004-R de 23 de junio de 2004, establece sobre los datos sensibles lo siguiente: «e) Derecho de exclusión de la llamada «*información sensible*» relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual[35]; información que potencialmente po-

---

[35] Sentencia 0189/2015 S3 de fecha 10 de agosto de 2015 establece III. FUNDAMENTOS JURÍDICOS DEL FALLO: «*La accionante alega la vulnera-*

dría generar discriminación o que podría romper la privacidad del registrado».

4.1.6 EL DERECHO A LA IMAGEN

La Constitución boliviana no consagra de manera expresa el derecho a la imagen, lo hace el Código Civil en el artículo 16, expresando que «Cuando se comercia, publica, exhibe o expone una imagen de

---

ción de sus derechos a la privacidad e intimidad, a la honra y honor, a la propia imagen, a la dignidad y a la autodeterminación informática, toda vez que el ahora demandado sin su autorización ni consentimiento, filmó una relación íntima que mantuvo con él, procediendo posteriormente a extorsionarla y amenazarla con difundirla, lo que en efecto se produjo el 1 de noviembre de 2013, siendo publicada por veintiún páginas web. En consecuencia, corresponde determinar si los extremos demandados son evidentes a efectos de conceder o denegar la tutela solicitada». POR TANTO: El Tribunal Constitucional Plurinacional, en su Sala Tercera; en virtud de la autoridad que le confiere la Constitución Política del Estado y el art. 12.7 de la Ley del Tribunal Constitucional Plurinacional; en revisión, resuelve: «… *2° CONCEDER la tutela respecto al Fiscal General del Estado y al Fiscal de Materia, Marco Patiño Serrano, sin responsabilidad por no haber sido demandados, ordenándose que dichas autoridades en uso de sus facultades y en cumplimiento de su rol de defensa del interés general de la sociedad, adopten las medidas de protección pertinentes a Paola Grisel Belmonte Gómez dentro del proceso penal que la misma inició contra Oscar Medinaceli Rojas, actual demandado. 3° Exhortar al Fiscal General del Estado que en su posición de garante –en razón a sus competencias- gestione y coordine con las instancias gubernamentales pertinentes las medidas necesarias para la implementación de programas de protección a las víctimas surgidas de plataformas virtuales y del internet; tomando en cuenta el deber de garantía hacia las víctimas, rol que constitucionalmente le está asignado como representante de la sociedad ante los órganos jurisdiccionales para velar por el respeto de los derechos y las garantías constitucionales, lo contrario sería no obedecer a su propósito como institución, e ir contra las normas constitucionales, generando en ese caso responsabilidades respecto de nuevas vulneraciones a los derechos referidos en este fallo constitucional. 4° Exhortar al Defensor del Pueblo para que en su rol asignado constitucionalmente de velar por la vigencia, promoción, difusión y cumplimiento de los derechos humanos, pueda hacer el seguimiento respectivo de la implementación y eficacia de las políticas de protección a las víctimas ejercidas por el Ministerio Público*».

una persona lesionando su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir, salvo los casos justificados por ley, que el juez haga cesar el hecho lesivo».

Sin embargo, su no consagración expresa, no impide que al tratarse de un hecho inherente a la persona, pueda encontrar protección a través de los recursos previstos en la Constitución, como lo ha entendido el Tribunal Constitucional en la Sentencia Constitucional 1376/2004-R al reconocer que el derecho a la imagen se deriva del derecho a la dignidad humana.

4.1.7 EL DERECHO A LA HONRA Y REPUTACIÓN

La jurisprudencia del Tribunal Constitucional, en la Sentencia Constitucional 686/2004-R, ha definido el derecho a la honra como: «… la estimación o deferencia con la que cada persona debe ser tenida y tratada por los demás miembros de la colectividad que le conocen; es el derecho que tiene toda persona a que el Estado y las demás personas reconozcan y respeten la trascendencia social de su honor. Es un derecho que se gana de acuerdo a las acciones realizadas por cada persona, de manera que en virtud de ellas pueda gozar del respeto y admiración de la colectividad como consecuencia de su conducta correcta e intachable acorde con valores de la ética y la moral, o por el contrario, carezca de tal imagen y prestigio, en razón de su indebido comportamiento social; cabe advertir que la honra, se constituye en una valoración externa de la manera como cada persona proyecta y presenta su imagen; de manera que las actuaciones buenas o malas, son el termómetro positivo o negativo que la persona irradia para que la comunidad se forme un criterio objetivo respecto de la honorabilidad de cada ser; pues las buenas acciones acrecientan la honra, las malas decrecen su valoración. En este último caso se entiende que no se puede considerar vulnerado el derecho a la honra de una persona, cuando es ella misma quien ha impuesto el desvalor a sus conductas y ha perturbado su imagen ante la colectividad».

Este derecho, si bien no estaba expresamente proclamado en el catálogo previsto por el artículo 7 de la abrogada Constitución de 1967, sí lo está en los artículos 12 de la Declaración Universal de Derechos Humanos, 5 de la Declaración Americana de Derechos y

Deberes del Hombre, 17 del Pacto Internacional de Derechos Civiles y Políticos, y 11 de la Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica.

La Sentencia Constitucional 0127/2010-R de 10 de mayo de 2010 establece que: «… el concepto de honra se debe construir desde puntos de vista valorativos y, en consecuencia, con relación a la dignidad de la persona. Desde dicha perspectiva la honra es un derecho de la esfera personal y se expresa en la pretensión de respeto que corresponde a cada persona como consecuencia del reconocimiento de su dignidad».

En Bolivia, la ley fundamental en armonía con las constituciones de otros países y los pactos internacionales, introdujo el instituto jurídico como una garantía constitucional destinada a tutelar los derechos a la intimidad y privacidad personal y familiar, a la imagen, honra y reputación.

4.2 LA ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

La nueva Constitución Política del Estado (CPE) ha sido aprobada mediante referéndum en fecha 25 de enero de 2009 que abroga la Constitución Política de 1967 y sus reformas posteriores.

En la Constitución promulgada en febrero de 2009 se ha ampliado el catálogo de los derechos civiles y políticos; es así que en el artículo 21.2) se han consagrado los derechos a la privacidad e intimidad, honra, honor, propia imagen y dignidad. En coherencia con ello, se ha consolidado la garantía constitucional jurisdiccional que protege el derecho a la intimidad y privacidad, en su dimensión positiva de conocer, objetar u obtener la eliminación o rectificación de los datos de la vida íntima o privada de la persona o sus familiares, mismos que son obtenidos, almacenados y distribuidos por bancos de datos públicos o privados por cualquier medio físico, electrónico, magnético e informático. Cabe advertir que, como parte del proceso de descolonización del Derecho, el Constituyente ha cambiado el nombre de la garantía constitucional jurisdiccional, denominándola Acción de Protección de Privacidad en reemplazo del Recurso de Hábeas Data (Rivera Santibáñez, 2010).

El Capítulo Segundo Derechos Fundamentales no reconoce expresamente en su articulado al derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación.

La vigente CPE considera a la Acción de Protección de Privacidad en el artículo 130 que en la abrogada CPE estaba establecida en el artículo 23 como Recurso de Hábeas Data y que establece:

> **Artículo 130.**
>
> I. «Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.
>
> II. La Acción de Privacidad no procederá para levantar el secreto en materia de prensa».

La Acción de Protección de Privacidad es un proceso constitucional de naturaleza tutelar que tiene por finalidad la protección inmediata y efectiva del derecho a la «autodeterminación informática», restableciendo o restituyéndolo en los casos en los que sea restringido o vulnerado de manera ilegal o indebida.

Rivera Santibáñez (2010:2) señala que: «la Acción de Protección de Privacidad es una garantía constitucional jurisdiccional que restituye o restablece de manera inmediata el derecho que tiene toda persona a verificar qué información o datos fueron obtenidos, o almacenados sobre ella, cuáles de ellos se difunden y con qué objeto, de manera que se corrijan o aclaren la información o datos inexactos, impedir que se difundan y, en su caso se eliminen si se tratan de datos o informaciones sensibles que lesionan su derecho a la vida privada o íntima en su núcleo esencial referido a la honra, la buena imagen o el buen nombre, en todos aquellos casos en los que los encargados de los bancos de datos públicos o privados vulneran el derecho al asumir la conducta ilegal o indebida de no permitir el acceso, la rectificación, la corrección, eliminación o mantenimiento en confidencialidad de los datos privados».

De lo referido se puede concluir que la Acción de Protección de Privacidad es una vía procesal de protección de los datos personales,

aquellos que forman parte del núcleo esencial del derecho a la privacidad o intimidad de una persona, frente a la obtención, almacenamiento y distribución ilegal, indebida o inadecuada por entidades u organizaciones públicas o privadas. Esta garantía constitucional otorga a toda persona, sea natural o jurídica, la potestad y facultad de acudir a la jurisdicción constitucional para demandar a los bancos de datos y archivos de entidades públicas y privadas con el fin de que le permitan el conocimiento, la actualización, la rectificación o supresión de las informaciones o datos referidos a ella, que hubiesen obtenido, almacenado y distribuido dichos bancos de datos (Rivera Santibáñez, 2010).

En la Sentencia Constitucional 1738/2010-R de fecha 25 de octubre de 2010 se cita a la autora Concepción Conde Ruiz, quién hace una distinción entre intimidad y privacidad, señalando que la intimidad es «el conjunto de sentimientos, pensamientos e inclinaciones más internos, como la ideología, religión o creencias, las tendencias personales que afectan a la vida sexual, problemas de salud que deseamos mantener en secreto y otras inclinaciones»; mientras que, privacidad hace referencia «al ámbito de la persona formado por su vida familiar, aficiones, bienes particulares y actividades personales».

De todo lo anterior se tiene que tanto la intimidad como la privacidad son la base fundamental para la protección de todos los datos personales del individuo, que sólo le atingen a él, por lo mismo se encuentra facultado para determinar cuándo y dentro de qué límites pueden revelarse situaciones referentes a su propia vida, entendiéndose en consecuencia de que la acción de protección de privacidad, entre otras protege la intromisión por parte de personas particulares y/o jurídicas a la vida íntima del ser humano que le corresponde como consecuencia del reconocimiento a su dignidad, por lo que la vulneración de estos derechos afectan directamente a su imagen, honra y reputación.

La Sentencia Constitucional 0189/2010-R de fecha 24 de mayo de 2010 establece: «… se tiene que los derechos fundamentales sustantivos como es el caso del derecho a la autotutela informativa, para su defensa necesitan medios o mecanismos idóneos para su protección. En efecto, en el contexto del Estado Social y Democrático de Derecho, máxime cuando se trate de la protección de datos administrados por entidades públicas, el Estado tiene la obligación de garan-

tizar ya sea por la vía administrativa o jurisdiccional, el resguardo pleno y eficaz de este derecho.

Por tanto, es evidente que el control de constitucionalidad a través de la garantía procesal-constitucional del Hábeas Data regulado por el artículo 23 de la abrogada CPE y denominado ahora Acción de Protección de Privacidad protegida por los artículos 130 y 131 de la CPE, no puede sustituir a estos mecanismos administrativos y jurisdiccionales y solamente debe ser activado en tanto y cuanto los mismos, una vez agotados, no restituyan el derecho a la «autotutela informativa» del afectado.

A partir del postulado antes señalado, y considerando que la naturaleza o esencia procesal constitucional de este instituto no ha cambiado con la entrada en vigor de la Constitución vigente, es pertinente señalar en principio que el hábeas data, ahora acción de protección de privacidad, es una garantía constitucional de naturaleza tutelar destinada a proteger el derecho a la «autotutela informativa», en tanto y cuanto no exista o no haya sido eficaz otro medio jurídico establecido para garantizar este derecho sustantivo, razón por la cual, se establece que la activación del control de constitucionalidad, a través de este mecanismo de defensa, de ninguna manera puede sustituir o ser alternativo a los mecanismos administrativos o jurisdiccionales establecidos para su protección, posición además sustentada por las SSCC 1572/2004-R, 1511/2004-R y 965/2004-R, entre otras».

4.2.1 DERECHOS QUE PROTEGE LA ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

En primer lugar, por la forma de redacción de la norma constitucional, pareciera que la acción tutelar protege un solo derecho; o dicho desde otra perspectiva, pareciera que la intimidad y privacidad, la imagen, honra y reputación fuesen un solo derecho fundamental. Al respecto cabe aclarar que no se trata de un solo derecho fundamental, sino de diferentes derechos:

a) El derecho a la intimidad y privacidad, que consisten en la capacidad, facultad o potestad de que tiene toda persona para mantener en reserva determinadas facetas de su personalidad referidas al

ámbito en el que se desenvuelve, su ámbito relacional y el de la manifestación de su voluntad.

b) El derecho a la imagen es la facultad o potestad que tiene toda persona de evitar la difusión incondicionada de su aspecto físico; se trata de un derecho que pretende salvaguardar un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás; un ámbito necesario para poder decidir libremente el desarrollo de la propia personalidad y, en definitiva, un ámbito necesario según las pautas de nuestra cultura para mantener una calidad mínima de vida humana. Cabe aclarar que se trata del derecho a proteger la imagen física y no de aquella otra que pretende definir el concepto que de una persona se tiene en el círculo social, económico o político que la circunda.

c) El derecho a la honra y reputación es la estimación o deferencia con la que cada persona debe ser tenida y tratada por los demás miembros de la colectividad que le conocen; es el derecho que tiene toda persona a que el Estado y las demás personas reconozcan y respeten la trascendencia social de su honor.

Lo que sucede es que el Constituyente, al consagrar los derechos fundamentales en el catálogo de la Constitución, los ha consignado en un mismo numeral 2) del artículo 21, cual si se tratase de un solo derecho fundamental, cuando se trata de diferentes derechos, como se ha descrito precedentemente.

En segundo lugar, con relación al derecho fundamental a la intimidad y privacidad, cabe recordar que este derecho tiene una doble dimensión. La Acción de Protección de Privacidad tutela o protege el derecho a la intimidad y privacidad en su *dimensión positiva*, vale decir, en la comprensión del derecho de acceder a los bancos de datos públicos y privados para conocer cuanta información o datos sobre su vida íntima y privada se han recogido y almacenado, conocer con qué finalidad se ha recogido y almacenado, y a quién o quienes se ha distribuido esa información o datos; lo que según la doctrina del Derecho Constitucional y del Derecho Procesal Constitucional supone la protección del derecho a la «autodeterminación informática». En consecuencia, la Acción de Privacidad no protege el derecho a la intimidad y privacidad en su *dimensión negativa*; vale decir, no protege el derecho a la inviolabilidad de domicilio, la inviolabilidad de comunicaciones privadas, y la inviolabilidad de documentos privados.

En tercer lugar, corresponde aclarar que la protección a los derechos a la imagen, la honra y reputación de la persona es muy particular de la configuración definida por el Constituyente boliviano, pues en la legislación comparada estos derechos no constituyen el objeto de protección o tutela del Recurso de Hábeas Data. Empero, se entiende que la protección a estos derechos está vinculada a la vulneración del derecho a la intimidad y privacidad en su dimensión positiva; lo que significa que no toda vulneración a los derechos a la imagen, la honra y la reputación activará la Acción de Protección de privacidad, sino que la misma tendrá lugar solamente en aquellos casos en los que, como consecuencia de la vulneración del derecho a la intimidad y privacidad en su dimensión positiva (derecho de autodeterminación informática) se vulneren esos derechos, causando daños y perjuicios a su titular o a su familia.

Finalmente, cabe aclarar que, considerando los elementos esenciales del derecho a la intimidad y privacidad en su dimensión positiva, la Acción de Protección de Privacidad protege a las personas permitiéndoles el acceso a los datos o informaciones obtenidas, almacenadas y distribuidas por los bancos de datos públicos o privados, para objetar, pedir su rectificación, su eliminación o supresión, con relación a los siguientes ámbitos de su vida privada:

a) El propio cuerpo, referido a la salud de la persona o de los miembros de su familia. Ello significa el derecho de una persona de mantener en reserva las afecciones de su salud o la de su familia, cuyo conocimiento podría menoscabar el juicio que, para fines sociales o profesionales, formulen las demás personas acerca del sujeto.

b) Las ideas y creencias religiosas, filosóficas, políticas, o sus ideas y pensamientos.

c) La vida pasada, relacionada a aquel ámbito que podría generarle bochorno al estar compuesta por pasajes desagradables o ingratos.

d) La vida doméstica, relacionada con aquellos hechos o situaciones que se producen dentro del hogar.

e) La vida familiar relacionada con el matrimonio y la filiación. Existen esferas que requieren ser mantenidas en reserva, por ejemplo la investigación de la paternidad, o el tema de las adopciones.

f) La vida amorosa y las relaciones de amistad, que incluye la vida sexual y, por extensión los embarazos prematrimoniales.

g) El ámbito de las comunicaciones personales, que comprende las diferentes vías de comunicación como las epistolares, telefónicas, electrónicas, fax, etc.

h) La situación económica personal, referidas al nivel de ingreso, patrimonio, inversiones, y obligaciones financieras (Rivera Santibáñez, 2010).

4.2.2 PROCEDIMIENTO PARA SU TRÁMITE

El artículo 131 de la Constitución Política del Estado de fecha 25 de enero de 2009, establece el procedimiento para la Acción de Protección de Privacidad.

I. «La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

II. Si el Tribunal o Juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

III. La decisión se elevará de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.

IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo a lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley».

Respecto al procedimiento que deberá emplearse para sustanciar la Acción de Protección de Privacidad el Constituyente reproduce el error cometido al haberse instituido el Recurso de Hábeas Data; toda vez que se remite a la aplicación supletoria del procedimiento previsto para la sustanciación de la Acción de Amparo Constitucional.

En efecto, la norma prevista por el art. 131.I de la Constitución textualmente dispone que «La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la Acción de Amparo Constitucional»; lo que significa que no tiene una configuración procesal propia, sino que se aplica la que fue prevista para la Acción de Amparo Constitucional.

La determinación del Constituyente no resulta correcta si se toma en cuenta que existe una diferencia entre la Acción de Protección de Privacidad y la Acción de Amparo Constitucional con relación a su naturaleza jurídica, sus fines y objetivos, así como sus alcances. En efecto, mientras la primera es una acción tutelar específica, la segunda es una general que protege los derechos y las garantías constitucionales consagrados ambos por la Constitución y las leyes, con excepción de aquellos que tienen una vía de protección específica; la primera tiene por finalidad el otorgar protección inmediata y efectiva al derecho a la intimidad y privacidad en su dimensión positiva, como es el derecho a la autodeterminación informática, en cambio la segunda tiene por finalidad otorgar la protección inmediata y efectiva a los derechos civiles, políticos, económicos, sociales y culturales (Rivera Santibáñez, 2010).

Finalmente, cabe señalar que mientras se mantuvo el procedimiento previsto para la Acción de Amparo Constitucional, el legislador retrasó el ejercicio de los derechos a conocer, objetar, obtener la eliminación o rectificación de los datos. La Acción de Protección de Privacidad tiene un propio procedimiento con la aprobación del nuevo Código Procesal Constitucional que será tratado más adelante.

4.2.3 EL CARÁCTER SUBSIDIARIO DE LA ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

En lo que respecta a su procedimiento, el artículo 131.I de la CPE establece que esta acción tendrá lugar de acuerdo con el procedimiento previsto para la Acción de Amparo Constitucional, de ahí que le son aplicables todos los requisitos de admisión y las causales de improcedencia del Amparo Constitucional, así como los principios de subsidiariedad e inmediatez.

En lo que respecta a la subsidiariedad la Sentencia Constitucional 0965/2004-R de fecha 23 de junio de 2004, señala: «Tomando en cuenta sus fines y objetivos, así como la aplicación supletoria de las normas previstas por el artículo 19 de la CPE, dispuesta por el artículo 23 parágrafo V antes referido, se entiende que el Hábeas Data es una acción de carácter subsidiario, es decir, que solamente puede ser viable en el supuesto que el titular del derecho lesionado haya reclamado ante la entidad pública o privada encargada del banco de datos, la entrega de la información o datos personales obtenidos o almacenados, y en su caso, la actualización, rectificación o supresión de aquella información o datos falsos, incorrectos, o que induce a discriminaciones, y no obtiene una respuesta positiva o favorable a su requerimiento, o sea que la entidad pública o privada no asume inmediatamente la acción solicitada. Dicho de otra manera, el Hábeas Data se activa exclusivamente cuando la persona demuestra que ha acudido previamente ante la entidad pública o privada para pedir la restitución de su derecho lesionado y no ha podido lograr la reparación a dicha vulneración».

En el mismo sentido, la Sentencia Constitucional 1572/2004-R de fecha 4 de octubre de 2004 señala que son aplicables al Hábeas Data los principios de subsidiariedad e inmediatez. De igual forma la Sentencia Constitucional 0188/2006-R de fecha 21 de febrero de 2006 establece el carácter subsidiario del hábeas data en los siguientes términos: «El artículo 23.V de la CPE, determina que el recurso de Hábeas Data «…se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el artículo 19° de esta Constitución»; consiguientemente, al Hábeas Data le es aplicable la doctrina constitucional sentada para el Amparo Constitucional, por lo que se debe aplicar el principio de subsidiariedad, establecido en el artículo 19.IV de la CPE; lo que significa que sólo se activa cuando el recurrente ha agotado los medios o recursos que tenía a su alcance para lograr conocer, objetar u obtener la eliminación, rectificación de los datos públicos o privados que afectan a su derecho a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación».

Sin embargo, cabe aclarar que, siguiendo la jurisprudencia constitucional establecida para la tramitación de la Acción de Amparo Constitucional respecto a la improcedencia por subsidiaridad, la regla admite una excepción; lo que supone que la Acción de Protección

de Privacidad podrá activarse excepcionalmente en aquellos casos en los que se lesione el derecho a la autodeterminación informática en su elemento del derecho a la confidencialidad o el derecho a la supresión de los datos o información de su vida privada e íntima; vale decir, cuando la persona titular del derecho pretende que se mantenga en confidencialidad o se suprima una información o dato personal considerado como sensible, cuya difusión podría causarle daños y perjuicios irreparables (Rivera Santibáñez, 2010).

De lo anterior se tiene que la Acción de Protección de Privacidad solo será procedente si se han agotado los recursos existentes y además se ha presentado la acción dentro del plazo de seis (6) meses.

4.3 DECRETO SUPREMO DE ACCESO A LA INFORMACIÓN DEL PODER EJECUTIVO

El Decreto Supremo 28168 de fecha 17 de mayo de 2005, tiene como objeto garantizar el acceso a la información como derecho fundamental de toda persona y la transparencia en la gestión del Poder Ejecutivo (artículo 1).

El acceso a la información pública, de manera oportuna, completa, adecuada y veraz es un requisito indispensable para el funcionamiento del sistema democrático y pilar fundamental de una gestión pública transparente, particularmente en el acceso a la información necesaria para investigar delitos de lesa humanidad, de violaciones a derechos humanos, delitos de daño económico al Estado y de hechos de corrupción.

El ámbito de aplicación del Decreto Supremo es el Poder Ejecutivo tanto a nivel central como descentralizado, autárquico y desconcentrado; empresas y sociedades del Estado y sociedades con participación estatal mayoritaria (artículo 2). El artículo 4 establece que se reconoce el derecho de acceso a la información a todas las personas como un presupuesto fundamental para el ejercicio pleno de la ciudadanía y fortalecimiento de la democracia.

En ejercicio de los derechos de información y petición, toda persona natural o jurídica, individual o colectivamente, está legitimada para solicitar y recibir información completa, adecuada, oportuna y veraz del Poder Ejecutivo (artículo 5). Las Máximas Autoridades Eje-

cutivas deben asegurar el acceso a la información a todas las personas sin distinción de ninguna naturaleza, estableciendo la estructura y procedimientos internos de las entidades públicas bajo su dependencia, que permitan brindar información completa, adecuada, oportuna y veraz (artículo 6).

El artículo 19 del Decreto Supremo 28168 de Acceso a la Información del Poder Ejecutivo de fecha 17 de mayo de 2005 establece:

I. «Toda persona, en la vía administrativa, podrá solicitar ante la autoridad encargada de los archivos y registros la actualización, complementación, eliminación o rectificación de sus datos registrados por cualquier medio físico, electrónico, magnético o informático, relativos a sus derechos fundamentales a la identidad, intimidad, imagen y privacidad. En la misma vía, podrá solicitar a la autoridad superior competente el acceso a la información en caso de negativa injustificada por la autoridad encargada del registro o archivo público.

II. La petición de hábeas data se resolverá en el plazo máximo de cinco (5) días hábiles. En caso de negativa injustificada de acceso a la información, la autoridad jerárquica competente, adicionalmente tendrá un plazo de quince (15) días hábiles para proporcionar la información solicitada.

III. La petición de hábeas data no reemplaza ni sustituye el Recurso Constitucional establecido en el artículo 23 de la Constitución Política del Estado[36]. El interesado podrá acudir, alternativamente, a la vía administrativa sin que su ejercicio conlleve renuncia o pérdida de la vía judicial. El acceso a la vía judicial no estará condicionado a la previa utilización ni agotamiento de esta vía administrativa».

Este Decreto Supremo establece un procedimiento para la vía administrativa del llamado «Hábeas Data Administrativo», acortando los plazos establecidos en el Decreto Supremo 27113 Reglamento de la Ley del Procedimiento Administrativo de fecha 23 de julio de 2003, procedimiento solamente válido para las entidades del sector público bajo dependencia del Poder Ejecutivo. También es interesante resaltar el desconocimiento del Decreto Supremo 28168 por parte de los servidores públicos y la ciudadanía en general.

---

[36] En la nueva CPE los artículos 130 y 131 Acción de Protección de Privacidad.

La jurisprudencia sentada por el Tribunal Constitucional a través de la Sentencia Constitucional 0188/2006-R establece que, «…el recurrente, antes de acudir a la vía jurisdiccional, debió agotar los recursos de revocatoria y jerárquico previstos en la Ley de Procedimiento Administrativo, lo que determina la improcedencia del recurso de hábeas data» [37].

La Sentencia 0189/2010-R de fecha 24 de mayo de 2010 establece: «… Asimismo, cuando el parágrafo tercero del art. 19 de la Ley 28168 [38], establece que, «… el interesado podrá acudir, alternativamente, a la vía administrativa sin que su ejercicio conlleve renuncia o pérdida de la vía judicial…»; y cuando establece también que, «… el acceso a la vía judicial no estará condicionado a la previa utilización ni agotamiento de esta vía administrativa…»; siguiendo el criterio de interpretación antes señalado y utilizando además un criterio de interpretación referente a la «unidad del ordenamiento jurídico», no puede interpretarse esta disposición como una alternatividad entre el «hábeas data administrativo» y la garantía constitucional del hábeas data, ya que tal como se dijo, para activar el control de constitucionalidad a través de este medio procesal-constitucional de defensa, previamente deben agotarse los mecanismos idóneos establecidos por ley; en ese contexto, el ejercicio del derecho a la «autotutela informativa» puede hacerse valer en la esfera administrativa y también en la esfera jurisdiccional ordinaria, a la cual el afectado puede acudir sin necesidad de agotar previamente la vía administrativa, aspectos que de ninguna manera alteran la esencia de la garantía constitucional del habeas data, ahora acción de protección de privacidad, que reiterando, solo puede ser activada cuando se haya agotado la vía administra-

---

37 Conforme el artículo 56.II de la Ley de Procedimiento Administrativo «los recursos administrativos proceden contra toda clase de resolución de carácter definitivo o actos administrativos que tengan carácter equivalente, siempre que dichos actos administrativos, a criterio de los interesados afecten, lesionen o pudieren causar perjuicio a sus derechos subjetivos o interese legítimos».

38 El Decreto Supremo 28168 no es Ley 28168, es un error de cita del Tribunal Constitucional Plurinacional debido a que la normativa se encuentra en el sitio web del Ministerio de Transparencia Institucional y Lucha contra la Corrupción como Ley 28168 de Acceso a la Información de 17 de mayo de 2005: http://www.transparencia.gob.bo/data/marco_legal/ds/ds28168.pdf [Consulta: 23/03/2015]

tiva o judicial pertinente, toda vez que le es aplicable el principio de subsidiaridad, tal como lo establecen las SSCC 1572/2004-R, 1511/2004-R y 965/2004-R, entre otras. Por lo expresado, se tiene que esta es precisamente la interpretación acorde a la Constitución que debe atribuírsele al art. 19.III de la Ley 28168».

Cabe señalar que las sentencias emitidas por el Juez de Partido o Tribunal de Hábeas Data han declarado improcedente el recurso por no haber agotado la vía administrativa, por lo que no es correcto decir que el acceso a la vía judicial no estará condicionado a la previa utilización ni agotamiento de la vía administrativa.

4.4 NUEVO CÓDIGO PROCESAL CONSTITUCIONAL

Cabe resaltar la aprobación del nuevo Código Procesal Constitucional de fecha 5 de julio de 2012, que establece un propio procedimiento para la Acción de Protección de Privacidad (ex Recurso de Hábeas Data) no utilizando por primera vez el procedimiento para la Acción de Amparo Constitucional como lo establecía la abrogada Constitución Política del Estado de 1967 (artículo 23, parágrafo V) y la vigente Constitución promulgada en febrero de 2009 (artículo 131.I).

El artículo 23 de la abrogada Constitución Política del Estado de 1967 establece:

> I. «El recurso de Hábeas Data se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el artículo 19 de esta Constitución».

Artículo 131 de la Constitución Política del Estado de 2009:

> I. «La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional».

El Capítulo Primero del Título II Acciones de Defensa establece el procedimiento común para las Acciones de Libertad, Amparo Constitucional, *Protección de Privacidad*, Cumplimiento y Popular:

— Reglas generales

— Improcedencia

— Comparecencia de terceros

— Competencia de juezas, jueces y tribunales

— Requisitos para la acción.

— Medidas cautelares
— Actuaciones previas
— Audiencia pública
— Contenido de la resolución
— Remisión al Tribunal Constitucional Plurinacional
— Responsabilidad y repetición
— Ejecución inmediata y cumplimiento de resoluciones
— Registro
— Sorteo
— Plazos para la resolución
— Formas de sentencia en acciones de defensa

El Capítulo Tercero establece el procedimiento específico para la Acción de Protección de Privacidad.

La Acción de Protección de Privacidad «tiene por objeto garantizar el derecho de toda persona a conocer sus datos registrados por cualquier medio físico, electrónico, magnético o informático, que se encuentre en archivos o bancos de datos públicos o privados; y a objetar u obtener la eliminación o rectificación de éstos cuando contengan errores o afecten a su derecho a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación» (artículo 58).

La novedad es la redacción positiva del artículo 58 sobre el reconocimiento al titular del dato el derecho a conocer, objetar, rectificar y obtener la eliminación de sus datos. El artículo 130 de la nueva CPE menciona «toda persona individual o colectiva que crea estar *indebida* o *ilegalmente impedida* de conocer, objetar u obtener la eliminación o rectificación de los datos registrados», lo cual se traducía en la práctica a que haya una respuesta negativa por parte de la Administración Pública o entidad del ámbito privado que detenta el archivo o base de datos para que el titular del dato pueda ejercer sus derechos de acceso, rectificación, cancelación y oposición, lo que implicaba el agotamiento de la vía administrativa antes de interponer la acción.

La Sentencia Constitucional 0071/2010-R de fecha 3 de mayo de 2010 establece: «… en el orden procesal en lo atinente a la terminología de esta acción tutelar, luego de un análisis se unificó criterios y se estableció que para referirse a la persona física o jurídica que in-

terponga esta acción tutelar será *«accionante»*, y con relación a la autoridad, funcionario, o persona contra quien se dirige esta acción corresponderá el término *«demandado (a)»*. De igual manera, en cuanto a la terminología con referencia a la parte dispositiva, en caso de otorgar la tutela se utilizará el término *«conceder»* y en caso contrario *«denegar»* la tutela. En los casos en que no sea posible ingresar al análisis de fondo de la problemática planteada, se mantendrá la denegatoria, haciéndose constar tal situación, dado que el accionante puede nuevamente interponer la acción tutelar, siempre y cuando, cumpla con los requisitos de admisibilidad».

La Acción de Protección de Privacidad puede ser interpuesta por:

1. «Toda persona natural o jurídica que crea estar afectada en su derecho, u otra persona a su nombre con poder suficiente.

2. Las herederas o herederos de una persona fallecida, que crean que ésta ha sido afectada en su derecho a la privacidad, imagen, honra y reputación, cuando dicho agravio genere directamente la vulneración de los derechos de ellas o ellos, en virtud del vínculo de parentesco con la difunta o difunto.

3. La Defensoría del Pueblo[39].

4. La Defensoría de la Niñez y Adolescencia[40]» (artículo 59).

---

[39] Constitución Política del Estado, artículo 218. I. La Defensoría del Pueblo velará por la vigencia, promoción, difusión y cumplimiento de los derechos humanos, individuales y colectivos, que se establecen en la Constitución, las leyes y los instrumentos internacionales. La función de la Defensoría alcanzará a la actividad administrativa de todo el sector público y a la actividad de las instituciones privadas que presten servicios públicos. II. Corresponderá asimismo a la Defensoría del Pueblo la promoción de la defensa de los derechos de las naciones y pueblos indígena originario campesinos, de las comunidades urbanas e interculturales, y de las bolivianas y los bolivianos en el exterior. III. La Defensoría del Pueblo es una institución con autonomía funcional, financiera y administrativa, en el marco de la ley. Sus funciones se regirán bajo los principios de gratuidad, accesibilidad, celeridad y solidaridad. En el ejercicio de sus funciones no recibe instrucciones de los órganos del Estado.

[40] La Defensoría de la Niñez y Adolescencia se crearon en 1997 para promover, proteger y defender los derechos de los niños, niñas y adolescentes. Las Defensorías fueron creadas por la Ley de Participación Popular 1551. Su funcionamiento está garantizado en el Código del Niño, Niña y Adolescente.

La Sentencia Constitucional 1978/2011-R de fecha 7 de diciembre de 2011 establece sobre la *legitimación activa* en la Acción de Protección de Privacidad: «Como una acción tutelar, el hábeas data sólo se activa a través de la legitimación activa restringida, la que es reconocida a la persona afectada, que puede ser natural o jurídica. En consecuencia, no admite una activación por la vía de acción popular, es decir, no se reconoce la legitimación activa amplia».

La jurisprudencia objeto del presente análisis establece dos elementos, el primero es que la persona afectada puede ser natural o jurídica, y el segundo elemento se refiere a la legitimación activa restringida; ambos condicen con lo establecido por el art. 130.I de la Constitución, por lo que esta jurisprudencia es compatible con la Constitución vigente. Entendimiento corroborado en los ordenamientos jurídicos de la órbita de nuestra cultura jurídica. El texto constitucional argentino de 1994 en su artículo 43.III, configurando la acción de hábeas data, como una modalidad del amparo, señala que: «Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados *destinados a proveer informes*, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos».

Respecto de la norma señalada, la doctrina concluye en cuanto a la legitimación activa, que dicha disposición habilita a toda persona a interponer la acción, es decir, puede plantearla tanto un individuo como una persona de existencia ideal, lo que no significa que se trate

---

Las Defensorías brindan a la comunidad un servicio municipal, permanente, público y gratuito. Aunque el costo de su funcionamiento es responsabilidad de los Gobiernos Municipales. En Bolivia, los niños, niñas y adolescentes han venido sufriendo, con demasiada frecuencia, maltrato, explotación, abandono y exclusión. Aunque el Estado había creado instancias para la protección de los derechos de la niñez y la adolescencia, estos mecanismos no eran efectivos. Para remediar la situación, se fundaron las Defensorías Municipales de la Niñez y la Adolescencia. Las Defensorías están compuestas por equipos interdisciplinarios. Abogados, trabajadores sociales, psicólogos y otros profesionales del área social conforman los equipos. De esta manera, las Defensorías brindan a los usuarios una atención integral. Los profesionales atienden casos de muy variada temática. Reciben denuncias de maltrato infantil, irresponsabilidad paterna y/o materna, explotación laboral, prostitución infantil, etc. (GAMSCZ, 2015).

de una activación por la vía de acción popular; por cuanto, sólo tiene legitimación el afectado por el banco o registro de datos en cuestión, así el artículo constitucional argentino subraya que el hábeas data es en pro de toda persona «para tomar conocimiento de los datos a ella referidos», o lo que es lo mismo, concernientes a la parte afectada en concreto, por cuanto la información a la que quiera acceder el solicitante debe referirse a cuestiones relacionadas con su interés, no pudiendo utilizarse por terceros sin derecho a hacerlo.

La Acción de Protección de Privacidad puede ser interpuesta contra:

1. «Toda persona natural o jurídica responsable de los archivos o bancos de datos públicos o privados donde se pueda encontrar la información correspondiente.

2. Toda persona natural o jurídica que pueda tener en su poder datos o documentos de cualquier naturaleza, que puedan afectar al derecho a la intimidad y privacidad personal, familiar o a la propia imagen, honra y reputación.

En ambos casos, tiene legitimación pasiva la persona natural o jurídica, pública o privada que compile datos personales en un registro, que independientemente de tener o no una finalidad comercial, esté destinado a producir informes, aunque no los circule o los difunda» (artículo 60).

La Sentencia Constitucional 1978/2011-R de fecha 7 de diciembre de 2011 establece sobre la *legitimación pasiva* «que recae precisamente sobre los bancos de datos (sean públicos o privados), que consisten en centros de acopio e intercambio de información, o de documentación, destinados a rubros específicos y a la prestación de determinados servicios (bancarios; policiales; comunicacionales; servicios web; compra y venta de distintos bienes; agencias matrimoniales; etc.), que estén expresamente destinados a brindar información a terceros. Por lo anteriormente descrito, los bancos de datos no comparten características similares a aquella información de carácter personal que una persona pueda tener en registros privados (computadoras, celulares, correos electrónicos, e-mails, y otros), debido a que son archivos que no tienen por objeto el de la publicidad del contenido de los mismos, es decir, no tienen por objeto el brindar información a terceros, por lo que no pueden ser objeto de tutela mediante la acción de protección de privacidad, en mérito a la naturaleza jurídica distinta a la de los bancos de datos y a que gozan de su protección consti-

tucional propia, establecida como la inviolabilidad del secreto de las comunicaciones privadas y los documentos y manifestaciones privadas contenidas en cualquier soporte (así lo establece el artículo 25.I y II[41] de la CPE), por lo que la acción destinada a proteger este tipo de derechos no es la acción de protección de privacidad, sino la acción de amparo constitucional, tal entendimiento establece que debe entenderse por banco de datos y cuáles serán los que pueden ser objeto de protección por esta acción tutelar».

Hay que esperar que establecerá la jurisprudencia del Tribunal Constitucional Plurinacional sobre el numeral 2) del parágrafo I del artículo 60 (Legitimación pasiva): «Toda persona natural o jurídica que pueda tener en su poder datos o documentos de cualquier naturaleza, que puedan afectar al derecho a la intimidad y privacidad personal, familiar o a la propia imagen, honra y reputación». El mencionado artículo hace referencia a que es sujeto a legitimación pasiva toda persona natural o jurídica que pueda tener «datos» o «documentos» de cualquier naturaleza, entiéndase que dato lo relacionaremos con «datos personales» que está definido en el artículo 3 (Definiciones) del Decreto Supremo 1793 Reglamento a la Ley 164 de 8 de agosto de 2011 para el Desarrollo de Tecnologías de Información y Comunicación aprobado en fecha 13 de noviembre de 2013 establece: «A los fines del presente Reglamento, se entiende como datos personales a toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable», como puede ser la imagen de una persona natural grabada mediante un celular, tableta, máquina fotográfica o computadora utilizados en el ámbito doméstico.

---

41 Artículo 25.- I. Toda persona tiene derecho a la inviolabilidad de su domicilio y al secreto de las comunicaciones privadas en todas sus formas, salvo autorización judicial. II. Son inviolables la correspondencia, los papeles privados y las manifestaciones privadas contenidas en cualquier soporte, éstos no podrán ser incautados salvo en los casos determinados por la ley para la investigación penal, en virtud de orden escrita y motivada de autoridad judicial competente. III. Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones o comunicaciones privadas mediante instalación que las controle o centralice. IV. La información y prueba obtenidas con violación de correspondencia y comunicaciones en cualquiera de sus formas no producirán efecto legal.

Por otra parte, el término «documentos» puede referirse a documentos en papel o documentos electrónicos o digitales. El autor mexicano Julio Téllez Valdés (2005:243) establece que en materia jurídica *documento* «es todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica». De acuerdo con este concepto, los documentos escritos no son la única manifestación de prueba documental, por lo que son documentos los planos gráficos, dibujos, fotografías, videos, películas, cintas magnetofónicas, discos informáticos, etc., que también se pueden constituir en última instancia, variedades de prueba documental. El documento digital está definido en el artículo 6 (Definiciones) en la Ley 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación como «…toda representación digital de actos, hechos o datos jurídicamente relevantes, con independencia del soporte utilizado para su fijación, almacenamiento o archivo».

Cabe señalar que la Sentencia Constitucional 1978/2011-R de fecha 7 de diciembre de 2011 establece que los bancos de datos no comparten características similares a aquella información de carácter personal que una persona pueda tener en registros privados (computadoras, celulares, correos electrónicos, e-mails, y otros), debido a que son archivos que no tienen por objeto el de la publicidad del contenido de los mismos, es decir, que no tienen por objeto el brindar información a terceros.

Por lo antes expuesto, se concluye que tiene legitimación pasiva la persona natural o jurídica que tenga en su poder datos o documentos de cualquier naturaleza (entendiéndose datos personales o documentos en soporte papel o electrónico contenidos en un dispositivo como celular, tableta, máquina fotográfica o computadora utilizados en el ámbito doméstico) que puedan afectar al derecho a la intimidad y privacidad personal, familiar o a la propia imagen, honra y reputación de la persona.

La Acción de Protección de Privacidad no procede cuando se ha interpuesto para levantar un secreto en materia de prensa, cuando hayan cesado los efectos del acto reclamado y cuando sea aplicable lo previsto en el artículo 53[42] del Código Procesal Constitucional (artículo 62).

---

[42] Artículo 53 (Improcedencia).- La Acción de Amparo Constitucional no procederá 1. Contra resoluciones cuya ejecución estuviere suspendida por efec-

Si el Órgano Jurisdiccional considera probada la violación del derecho, puede establecer la existencia de indicios de responsabilidad civil o penal de la accionada o accionado de conformidad al artículo 39[43] del Código Procesal Constitucional[44].

---

to de algún medio de defensa o recurso ordinario o extraordinario interpuesto con anterioridad por el recurrente, y en cuya razón pudieran ser revisadas, modificadas, revocadas o anuladas; 2. Contra actos consentidos libre y expresamente, o cuando hayan cesado los efectos del acto reclamado; 3. Contra resoluciones judiciales o administrativas que pudieran ser modificadas o suprimidas por cualquier otro recurso, del cual no se haya hecho uso oportuno; 4. Cuando la omisión de la Servidora o Servidor Público, vulnere un mandato expreso de la Constitución Política del Estado o la Ley, tutelado por la Acción de Cumplimiento; y 5. Cuando los derechos o garantías vulnerados correspondan ser tutelados por las Acciones de Libertad, de Protección de Privacidad o Popular.

43 Artículo 39 (Responsabilidad y repetición).- I. La resolución que conceda la acción, podrá determinar también, la existencia o no de indicios de responsabilidad civil o penal, estimando en el primer supuesto el monto a indemnizar por daños y perjuicios y en el segundo, remitiendo antecedentes al Ministerio Público y a la Procuraduría General del Estado cuando corresponda. A este efecto el Tribunal podrá abrir un término de prueba de hasta diez días, computables a partir de la notificación en la misma audiencia. II. Si la responsabilidad fuera atribuible a una servidora o servidor público, la Jueza, Juez o Tribunal que concedió la acción, ordenará la remisión de una copia de la resolución a la máxima autoridad administrativa de la entidad donde preste sus servicios, para el inicio, si corresponde, del proceso disciplinario.

44 Sentencia Constitucional 1738/2010-R de fecha 25 de octubre de 2010 establece III. FUNDAMENTOS JURÍDICOS DEL FALLO: *«La recurrente ahora accionante denuncian la vulneración de los derechos de su representada a la privacidad, dignidad, intimidad, decoro, honor y a la «seguridad jurídica», aduciendo que su representada menor de edad V.G.Z., tuvo una relación íntima con su ex enamorado ahora demandado, quien mediante un aparato celular procedió a filmar parte de la relación sexual, la cual posteriormente circuló en la página web Bolivia.com, así como en los aparatos celulares de los alumnos y docentes de la universidad donde estudiaba, por lo que ante este daño moral, psicológico, espiritual, emocional que va contra la dignidad, personalidad, decoro y fundamentalmente la intimidad de su representada, se vio obligada a impedir que continúe asistiendo a la universidad, por la serie de comentarios y discriminaciones de la que fue objeto no sólo su representada sino toda su familia, máxime si su actividad laboral es de maestra normalista del nivel secundario. Consiguientemente, en revisión de la Resolución del Tribunal de garantías corresponde determinar si se*

Si la acción fuese promovida por un acto ilegal o indebido, que impida conocer, objetar, eliminar o rectificar los datos registrados por cualquier medio físico, electrónico, magnético o informático en archivos o bancos de datos públicos o privados, la sentencia ordenará la revelación de los datos cuyo registro fuera impugnado (artículo 63).

4.4.1 INTERPOSICIÓN DIRECTA DE LA ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

Cabe resaltar que otra novedad importante es la establecida en el artículo 61 que señala que puede interponerse de forma directa, sin necesidad de reclamo administrativo previo por la inminencia de la violación del derecho tutelado y la acción tenga un sentido eminentemente cautelar.

No obstante, la misma jurisprudencia constitucional ha establecido que es posible aplicar la excepción a la regla de la subsidiaridad en situaciones en las que los hechos ilegales o indebidos denunciados en una acción de protección de privacidad podrían producir efectos irreparables o irremediables; de manera que, a pesar de existir vías legales ordinarias para que los accionantes puedan lograr la restitución de sus derechos fundamentales restringidos o suprimidos es posible activar inmediatamente esta vía tutelar para que, compulsando los antecedentes y verificando que los hechos ilegales o indebidos denunciados lesio-

---

debe otorgar o no la tutela impetrada». POR TANTO: *«El Tribunal Constitucional, en virtud de la jurisdicción y competencia que le confieren los arts. 4 y 6 de la Ley 003 de 13 de febrero de 2010, denominada Ley de Necesidad de Transición a los Nuevos Entes del Órgano Judicial y Ministerio Público; 7 inc. 8) y 102.V de la Ley del Tribunal Constitucional, en revisión, resuelve: 1.º APROBAR la Resolución de 001/2007 de 12 de noviembre, cursante de fs. 28 a 30, pronunciada por la Sala Penal de la Corte Superior del Distrito Judicial de Beni; y en consecuencia, CONCEDE la tutela solicitada, en los términos dispuestos por el Tribunal de garantías. 2.º De conformidad a lo previsto por el art. 102.II de la CPE, se dispone responsabilidad civil y penal contra el demandado Oscar Yasmani Justiniano Egües, a cuyo efecto el Tribunal de garantías en ejecución de sentencia fijará el monto por los daños y perjuicios ocasionados; las medidas y acciones pertinentes para su cumplimiento, como también deberá remitir antecedentes al Ministerio Público para el respectivo procesamiento penal».*

naron los derechos fundamentales, cuyos efectos podrían ser irreparables o irremediables, se otorgue una tutela provisional o directa.

Para ese efecto, este Tribunal Constitucional, a través de su jurisprudencia, ha establecido las respectivas subreglas que permitan determinar de manera objetiva el peligro del perjuicio irreparable o irremediable; así, en su Sentencia Constitucional 1743/2003-R de fecha 1 de diciembre de 2003 señala que: «Para determinar la irremediabilidad del perjuicio hay que tener en cuenta la presencia concurrente de varios elementos que configuran su estructura, como la inminencia, que exige medidas inmediatas, la urgencia que tiene el sujeto de derecho por salir de ese perjuicio inminente, y la gravedad de los hechos, que hace evidente la impostergabilidad de la tutela como mecanismo necesario para la protección inmediata de los derechos constitucionales fundamentales. La concurrencia de los elementos mencionados pone de relieve la necesidad de considerar la situación fáctica que legitima la acción de tutela como mecanismo transitorio y como medida precautelativa para garantizar la protección de los derechos fundamentales que se lesionan o que se encuentran amenazados. Con respecto al término «amenaza» es conveniente manifestar que no se trata de la simple posibilidad de lesión, sino de la probabilidad de sufrir un mal irreparable y grave de manera injustificada. La amenaza requiere un mínimo de evidencia fáctica, de suerte que sea razonable pensar en la realización del daño o menoscabo material o moral.

De acuerdo con lo que se ha esbozado sobre el perjuicio irremediable, se deduce que hay ocasiones en las que, de continuar las circunstancias de hecho en que se encuentra una persona, es inminente e inevitable la destrucción grave de un bien jurídicamente protegido, de manera que urge la protección inmediata e impostergable por parte del Estado ya en forma directa o como mecanismo necesario para la protección inmediata de los derechos constitucionales fundamentales. La concurrencia de los elementos mencionados pone de relieve la necesidad de considerar la situación fáctica que legitima la acción de tutela, como mecanismo transitorio y como medida precautelativa para garantizar la protección de los derechos fundamentales que se lesionan o que se encuentran amenazados».

La Sentencia Constitucional 1445/2013 de fecha 19 de agosto de 2012 establece que: «el artículo 61 del CPC establece una excepción al principio de subsidiariedad de esta acción tutelar, cuando se-

ñala que la acción de protección de privacidad podrá interponerse de forma directa, sin necesidad de reclamo administrativo previo, por la inminencia de la violación del derecho tutelado y la acción tenga un sentido eminentemente cautelar.

De donde se concluye que previo a acudir ante la jurisdicción constitucional, de manera general, se debe actuar conforme dispone la jurisprudencia, es decir, reclamar ante la entidad pública o privada encargada del resguardo y administración de la información, la entrega, actualización, rectificación o supresión de la información o datos falsos, incorrectos o que induce a discriminaciones; y en caso de no obtener una respuesta positiva favorable a su petitorio, y por ende, la reparación de sus derechos, entonces recién quedará expedita la vía constitucional; sin embargo, de acuerdo al texto contenido en el precitado artículo 61 del Código Procesal Constitucional, podrá hacerse abstracción de la aplicación del principio de subsidiariedad, en virtud a lo cual no se exigirá el reclamo administrativo previo, por la inminencia de la violación del derecho tutelado y la acción tenga un sentido eminentemente cautelar.

No se debe perder de vista que para que sea viable la excepción alegada, se deben cumplir de manera simultánea ambos requisitos, dado que se encuentran unidos por la conjunción copulativa «y», que denota el vínculo o nexo entre ambas, e implica que deben darse a la vez, es decir, se evidencia la inminente de la violación al derecho a la autotutela informativa, lo que se traduce en que exista una extrema proximidad de una lesión o vulneración, y el mecanismo de defensa pretenda evitar daños y perjuicio irreparables, como una medida preventiva».

La Sentencia Constitucional 0189/2015 S3 de fecha 10 de agosto de 2015 establece: «… Ahora bien cabe referirnos al artículo 61 del Código Procesal Constitucional, que prevé que la acción de protección de privacidad podrá interponerse ante la «… inminencia de la violación del derecho tutelado…» denotando además su sentido estrictamente cautelar, no obstante y en base a lo referido previamente, cabe diferenciar entre *tutela transitoria* y *tutela inmediata*, siendo que la primera procederá en caso que exista otro mecanismo para la protección del derecho, pero que ante la gravedad e inminencia de la vulneración será necesario acudir a la misma, requisito que no es atendible en nuestro caso al constatar que no existe mecanismo alguno con el que la víctima pueda contar en un proceso penal como el que nos ocupa en el

presente, por su parte la tutela inmediata responde a la inminencia de vulneración del hecho tutelado, lo cual se evidencia en el caso concreto, por lo que corresponde aplicar de manera directa la tutela inmediata en base al fundamento *ut supra* referido. Sin embargo, cabe aclarar que la aplicación de la tutela transitoria e inmediata de la acción de protección de privacidad, dependerá siempre de cada caso concreto y responderá a la evaluación de los antecedentes y supuestos fácticos para determinar si procede o no la interposición directa».

4.5 EL TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO SANITARIO BOLIVIANO

4.5.1 CÓDIGO DE SALUD DE LA REPÚBLICA DE BOLIVIA

El Código de Salud, aprobado en fecha 18 de julio de 1978, está conformado por seis (6) libros y ciento cincuenta y seis (156) artículos y un Título Preliminar.

La finalidad del Código de Salud es la regulación jurídica de las acciones para la conservación, mejoramiento y restauración de la salud de la población mediante el control del comportamiento humano y de ciertas actividades, a los efectos de obtener resultados favorables en el cuidado integral de la salud de los habitantes de la República de Bolivia (artículo 1).

El artículo 2 señala que «la salud es un bien de interés público, corresponde al Estado velar por la salud del individuo, la familia y la población en su totalidad».

También establece el derecho a la salud de todo ser humano que habite el territorio nacional sin distinción de raza, credo político, religión y condición económica y social, derecho que es garantizado por el Estado (artículo 4).

En relación a los establecimientos que prestan servicios de salud, el Código de Salud señala: «la Autoridad de Salud, en coordinación con el organismo nacional competente dictará las normas técnicas y administrativas sobre la organización, instalación, autorización, funcionamiento, planta física de personal necesario mínimo, planta física y diseño de planes del edificio, ubicación, instalaciones y otras espe-

ciales conforme a la naturaleza y magnitud de los establecimientos que prestan servicios de salud, sean estos públicos o privados, incluyendo los consultorios privados» (artículo 134).

Para la instalación y funcionamiento de un establecimiento que presta servicios de salud a las personas, trátese de hospitales, clínicas, laboratorios, consultorios, gabinetes de diagnóstico y tratamiento y cualquier otro establecimiento similar, deberá previamente obtener su autorización, aprobación de planes y registro ante la Autoridad de Salud, acreditando haber cumplido los requisitos establecidos por normas técnicas y administrativas. Las Autorizaciones administrativas serán concedidas por tiempo limitado prorrogable (artículo 135).

La Sanidad Internacional está sujeta a las normas contenidas en los Tratados y Convenios de los que forman parte la República de Bolivia, a las del Código de Salud y las reglamentarias que dicte la Autoridad de Salud (artículo 139).

La Autoridad de Salud, en coordinación con el Instituto Nacional de Estadística, establecerá el Sistema Nacional de Información en Estadística de Salud como parte integrante del Sistema Nacional de Estadística (artículo 143).

Todas las instituciones que realizan acciones relacionadas con salud, directa o indirectamente, sean estas públicas o privadas, están sometidas al cumplimiento de las normas de organización y producción que emanen del organismo central del Sistema Nacional de Estadística de Salud (artículo 144). Las instituciones de salud, tanto públicas como privadas, así como los profesionales en ejercicio y toda persona natural o jurídica que realicen acciones de salud, están obligados a informar los datos sobre estadísticas sanitarias y administrativas que les señale la Autoridad de Salud conforme a las disposiciones que sean dictadas (artículo 145).

4.5.2 DECRETO SUPREMO 18886 REGLAMENTOS CONCERNIENTE AL CÓDIGO DE SALUD

El Decreto Supremo 18886 de fecha 15 de marzo de 1982 aprueba los Reglamentos que a continuación se detallan concernientes al Código de Salud aprobado mediante Decreto ley 15629 de fecha 18 de julio de 1978:

— Farmacias y laboratorios.
— Establecimientos de Salud Públicos y Privados.
— Establecimientos de Salud Privados.
— Especialidades Médicas.
— Ejercicio de la Enfermería.
— Otros.

4.5.2.1 Reglamento de Establecimientos de Salud Públicos y Privados

Se entiende por Establecimientos de Salud a los hospitales, cualesquiera sean su tamaño o especialidad, públicos o privados, policlínicos, Centros de Salud, Hospitales, Puestos Médicos, Puestos Sanitarios, Clínicas y Consultorios Privados y todo aquel en el que se realizan actividades concernientes a la salud de las personas (artículo 10).

La finalidad de los establecimientos de salud es la de proveer a las personas servicios integrales que tiendan a prevenir las enfermedades, promover la salud, reparar las enfermedades y rehabilitar a los impedidos, así como servir de centros de investigación y de enseñanza para la formación de los recursos humanos que requiere Bolivia (artículo 11).

Los hospitales deben organizar sus servicios en tres (3) Departamentos:

a) Departamento de servicios médicos
b) Departamento de servicios técnicos
c) Departamento de servicios administrativos

En hospitales generales de tipo A:

Departamento Servicios Médicos	Departamento Servicios Técnicos	Departamento Servicios Administrativos
Medicina	Laboratorio	Administración Financiera
Cirugía	Radiología	Personal
Obstetricia – ginecología	Farmacia	Compras y suministros
Pediatría	Enfermería	Mantenimiento

Departamento Servicios Médicos	Departamento Servicios Técnicos	Departamento Servicios Administrativos
Anestesiología	Archivo Clínico	Servicios Generales
Consultorio externo		
Emergencia		

En los hospitales generales de tipo B:

Departamento Servicios Médicos	Departamento Servicios Técnicos	Departamento Servicios Administrativos
Consultorio externo	Rayos X	Admisión – información
Medicina general	Farmacia	Administración
Cirugía general	Laboratorio	Contabilidad
Anestesiología	Banco de sangre	Personal
Pediatría	Enfermería	Almacenes
Obstetricia y ginecología	Dietética	Mantenimiento
Enfermedades infecto – contagiosas	Archivo clínico	Lavandería
Traumatología y orto-pedia	Servicio social	Aseo y limpieza
Odontología	Educación en salud	
Emergencias		
Medicina preventiva		

En los hospitales generales de tipo C:

Departamento Servicios Médicos	Departamento Servicios Técnicos	Departamento Servi-cios Administrativos
División de Medicina	Rayos X	Información
Medicina general	Farmacia	Admisión
Enfermedades infecto – contagiosas	Laboratorio clínico	Administración
Cardiología	Banco de sangre	Contabilidad
Dermatología	Enfermería	Personal
Gastroenterología	Fisioterapia	Almacenes
Cancerología	Dietética y nutrición	Mantenimiento

Departamento Servicios Médicos	Departamento Servicios Técnicos	Departamento Servicios Administrativos
Endocrinología	Servicio social	Lavandería
Neurología	Docencia e investigación	Aseo y limpieza
Enfermedades metabólicas	Saneamiento ambiental	Transportes
Medicina preventiva	Educación sanitaria	Ropería y costura
Consultorio externo	Archivo clínico	Vigilancia
Electroencefalografía	Servicios religiosos	
Electrocardiografía	Otros servicios	
División de Cirugía		
Cirugía general Anestesiología		
Traumatología y ortopedia		
Oftalmología		
Otorrinolaringología		
Urología		
Odontología		
Cirugía plástica		
Neurocirugía		
Anatomía patológica		
Emergencias		
División Pediatría		
Clínica pediátrica		
Cirugía pediátrica		
Neonatología		
División de Gineco – Obstetricia		
Obstetricia		
Ginecología		

Fuente de elaboración: Propia en base al Reglamento de Establecimientos de Salud Públicos y Privados.

4.5.2.2 Reglamento de Establecimientos de Salud Privados

Se entienden por clínica particular a un establecimiento destinado a prestar servicios médicos a pacientes hospitalizados y ambulatorios.

Se entiende por otros establecimientos de salud, los consultorios médicos generales o de especialidades, los consultorios odontológicos y todos aquellos establecimientos que debido a su naturaleza están relacionados con la salud, como ser los servicios de emergencia, enfermería, establecimientos de Optometría, Laboratorios Dentales, Rehabilitación, Fisioterapia, Centros de Dictoterapia y Adelgazamiento, atendidos por profesionales en el campo de la salud, debiendo el Ministerio de Previsión Social y Salud Pública determinar cuáles otros establecimientos deben ser considerados para los efectos del Reglamento (artículo 1).

Por el número de camas, los establecimientos de salud de propiedad privada se clasifican en:

— Clínicas de tipo A de 10 a 25 camas.

— Clínicas de tipo B de 26 a 50 camas.

— Clínicas de tipo C de más de 51 camas.

Por la calidad de su infraestructura, equipamiento y de sus recursos humanos, así como por el cumplimiento de las normas estipuladas en el Estatuto General de Hospitales y el Reglamento de Establecimientos de Salud Privados pueden ser de tipo A, B o C (artículo 2).

El personal paramédico estará establecido o determinado de acuerdo con la complejidad de servicios y el número de camas.

a) Las Clínicas de tipo A deben contar con laboratorio clínico; asimismo, tendrán los medios indispensables para realizar transfusiones sanguíneas en caso de emergencia. En cuanto a radiodiagnóstico, contarán por lo menos con un equipo portátil de Rayos X.

b) Las Clínicas de tipo B deben disponer de un laboratorio Clínico y Banco de Sangre; en cuanto a radiodiagnóstico, contará por lo menos con un equipo de Rayos X de 250 m.a.

c) Las Clínicas de tipo C están obligadas a contar con Laboratorio Clínico y Banco de Sangre completos.

d) Los servicios auxiliares de diagnóstico de las clínicas de tipo A, B, C, deberán prestar atención permanente incluso los domingos, feriados y en horas de la noche.

e) Toda clínica privada deberá contar con un sistema adecuado de eliminación de desechos sólidos.

f) De igual manera, deberá contar con una lavandería propia dentro de su recinto y disponer de medios de esterilización de ropa contaminada.

g) Toda Clínica de medicina general deberá contar, por lo menos, con un equipo de resucitación, incluyendo el desfibrilador cardiaco. En caso de atención infantil, estas deben disponer de incubadoras.

h) Tendrán también un adecuado sistema de esterilización instrumental y equipo de uso médico (artículo 6).

La apertura y funcionamiento de establecimientos de salud será autorizado mediante Resolución Ministerial previo cumplimiento de los requisitos correspondientes (artículo 4).

a) Todo establecimiento deberá llevar de forma obligatoria los siguientes registros:

1. Un libro de Registro diario de ingresos y altas de pacientes.
2. Historia clínica de cada paciente de acuerdo a normas.
3. …
4. Contará con un archivo de historial clínico de los pacientes atendidos.

b) De todas las actividades realizadas, mensualmente se enviará una copia a la Regional de Salud correspondiente para su procesamiento, con especificación de ingresos y altas de pacientes, natalidad, mortalidad, intervenciones quirúrgicas y cualquier otra actividad realizada por la clínica.

c) Las enfermedades de notificación obligatoria deberán ser denunciadas de acuerdo a normas establecidas… (artículo 9).

4.5.2.3 **Reglamento de Especialidades Médicas**

Se reconocen las especialidades médicas como capítulos específicamente definidos en las prácticas de la medicina a fin de conseguir un adecuado ordenamiento en el ejercicio de las mismas y una mejor prestación de servicios a la comunidad (artículo 2).

Los médicos especialistas deben registrarse en el Ministerio de Previsión Social y Salud Pública, previo trámite ante el Colegio Médico de Bolivia a través de las Sociedades Médicas Especialidades reco-

nocidas por el Cuerpo Colegiado, las que calificarán los documentos y le asignarán la calificación de especialista reunidos los requisitos que tengan establecidos (artículo 3).

Solo se reconocen especialidades cuyo currículum puede homologarse a los programas vigentes en las Facultades de Medicina de Bolivia (artículo 4).

Se reconocen las siguientes especialidades (artículo 5):

Medicina Interna	
Cardiología	Reumatología
Endocrinología	Nefrología
Gastroenterología	Neurología
Hematología	Inmuno-Alergología
Hematología	Infectología
Neumología	Dermatología
Deportología	Patología Tropical
Ginecología – (Obstreticia) Obstetricia	
Ginecología	
Obstetricia	
Pediatría	
Pediatría Clínica	
Pediatría Quirúrgica	
Salud Pública	
Cirugía	
General	Oftalmología
Ortopedia y Traumatología	Anestesiología
Cardio-vascular	Proctología
Cirugía de Tórax	Urología
Otorrinolaringología	Angiología
	Plástica y Reparatoria
Otras Especialidades	
Psiquiatría	
Radiología	

Otras Especialidades
Anatomía Patológica
Oncología
Medicina Nuclear
Medicina Legal
Laboratorio Clínico

Fuente tabla: Elaboración propia.

4.5.2.4 Reglamento del ejercicio de la Enfermería

El concepto de enfermería, como una de las profesiones de la salud, debe proporcionar una atención de enfermería de calidad y contribuir así a elevar a nivel de salud y bienestar de la población en el proceso de desarrollo social. Como tal, forma parte del sistema de salud y se interesa en la solución de los problemas que afectan a la sociedad que es dinámica; motivando que esta profesión adopte su doctrina, su función y servicios de acuerdo a las transformaciones sociales y demanda de cobertura (artículo 1.º).

Enfermería es la prestación de servicios a individuos, familia y colectividad para el restablecimiento o preservación de la salud, siendo la cantidad y calidad de cuidados, factores importantes que contribuyen al mejoramiento y a la extensión de servicios a la población (artículo 2.º).

Sobre las categorías del personal de enfermería están:

a) Enfermera o enfermero es la persona que, habiendo cumplido un programa de educación y formación básica en enfermería a cargo de una institución de enseñanza reconocida por el Supremo Gobierno, esté calificada y autorizada para ejercer servicios profesionales que requieren responsabilidad y competencia en el campo de la prevención, recuperación y rehabilitación de la salud (artículo 3.º).

b) Auxiliar de Enfermería es la persona preparada mediante un programa educativo en técnicas auxiliares de enfermería, reconocida oficialmente para participar bajo la dirección y supervisión de la enfermera en actividades del servicio de salud (artículo 4.º).

c) Enfermera por años de servicio es la persona que no habiendo seguido ningún curso académico de enfermería optó por el diploma que la acredita como Enfermera Titular al amparo de la ley de 30 de diciembre de 1948 (artículo 5.º).

En relación a la moral de la enfermería, señala el inciso e) Sólo a requerimiento judicial o de autoridad pertinente las enfermeras profesionales, titulares o auxiliares de enfermería podrán romper el secreto profesional. En caso de enfermedades transmisibles comunicarán a las autoridades pertinentes (artículo 62.º).

Son actos contrarios a la honradez y en consecuencia condenables por la ética:

a) Efectuar comentarios que perjudiquen a pacientes, familiares, personal de enfermería, instituciones, facultativos y superiores.

b) Sólo a requerimiento judicial o de autoridad pertinente las enfermeras profesionales o auxiliares de enfermería, podrán romper el secreto profesional.

En caso de enfermedades transmisibles, las enfermeras comunicarán a las autoridades pertinentes (artículo 63).

4.6 LEY DEL EJERCICIO PROFESIONAL MÉDICO

La Ley 3131 del Ejercicio Profesional Médico aprobada en fecha 8 de agosto de 2005, se constituye en el marco regulatorio del hacer médico, cumpliendo sus tareas bajo los preceptos de sus derechos y obligaciones. Esta ley fue aprobada a consecuencia de que en los últimos tiempos, por infortunios en el desempeño de su profesión, los médicos fueron acusados de «negligencia médica».

La Ley 3131 tiene como objeto regular el Ejercicio Profesional Médico en Bolivia. Su ámbito de aplicación es el Sistema Nacional de Salud, conformado por los sectores: Público, Seguridad Social, Privado sin fines de lucro y Privado con fines de lucro, legalmente autorizados.

Tiene como principios:

— La profesión médica está consagrada a la defensa de la vida, cuidado de la salud integral de la persona, familia y comunidad.

— El médico ejerce una labor en el marco de la probabilidad de toda ciencia para obtener resultados probables.

— El médico en el ejercicio de su profesión debe actuar con autonomía e independencia, guiado por normas y protocolos vigentes.

— En el ejercicio profesional médico, inclusive en la enseñanza de la medicina, *el secreto médico* es inviolable salvo las excepciones previstas en la Ley 3131 (artículos 1, 2 y 3).

4.6.1 ORGANIZACIONES MÉDICAS

La Ley 3131 establece como Entidad Colegiada al Colegio Médico de Bolivia como máxima entidad organizacional, científica, gremial y de perfeccionamiento profesional del cuerpo médico.

El Ministerio del área de Salud es el responsable de la supervisión y control del ejercicio profesional médico en coordinación con el Colegio Médico de Bolivia (artículos 5 y 6).

4.6.2 EJERCICIO MÉDICO Y LAS FUNCIONES

Para el ejercicio profesional, el médico debe estar matriculado en el Ministerio del área de Salud (artículo 7).

El Ejercicio profesional médico tiene como funciones:

— Promoción de la salud.

— Prevención de la enfermedad.

— Recuperación de la salud.

— Rehabilitación del paciente (artículo 8).

Bajo el resguardo y custodia del establecimiento de salud, son de uso exclusivo del médico los Documentos Médicos oficiales, siendo considerados como tales los siguientes:

a) Expediente médico.

b) Historia clínica.

c) Consentimiento informado.

d) Informes de procedimientos auxiliares de diagnóstico y tratamiento.

e) Certificado médico.

f) Informes médicos.
g) Certificado de mortinato.
h) Certificado de nacido vivo.
i) Certificado de defunción.
j) Protocolo de autopsia.
k) Informe pericial.
l) Hoja anestésica.
m) Interconsultas.
n) Descripción del procedimiento quirúrgico.
o) Epicrisis.
p) Transferencias.
q) Informes médicos legales.
r) Recetas médicas (artículo 10).

4.6.3 DERECHOS Y DEBERES DEL MÉDICO

Dentro de los deberes del médico, establecidos en el artículo 12 de la Ley 3131, se rescatan los relacionados con la información, consentimiento del paciente, secreto médico.

— Respetar el *consentimiento expreso del paciente*, cuando rechace el tratamiento u hospitalización que se le hubiera indicado.
— *Informar al paciente*, o responsables legales, con anterioridad a su intervención, sobre los riesgos que pueda implicar el acto médico.
— Guardar el *secreto médico*, aunque haya cesado la prestación de sus servicios.

4.6.4 **DERECHOS Y DEBERES DEL PACIENTE**

Se destacan los derechos de los pacientes relacionados con el tratamiento de los datos de salud establecidos en el artículo 13 de la Ley 3131:

a) La confidencialidad.
b) Secreto médico.

c) Recibir información adecuada y oportuna para tomar decisiones libre y voluntariamente.

d) Reclamar y denunciar si considera que sus derechos humanos han sido vulnerados durante la atención médica.

e) Respeto a su intimidad.

Asimismo, dentro de los deberes del paciente, éste debe comunicar de manera veraz y completa sus antecedentes de salud, personales y familiares (artículo 14).

4.6.5 AUDITORÍA MÉDICA

La auditoría médica es un procedimiento técnico analítico, evaluativo, de carácter preventivo y correctivo, con el fin de emitir un dictamen, informe o certificación independiente referente al acto médico y a la gestión de calidad de los servicios de salud.

La auditoría médica es realizada exclusivamente por profesionales médicos debidamente acreditados, como auditores médicos avalados por el Ministerio del área de Salud en coordinación con el Colegio Médico de Bolivia, con el apoyo de otros profesionales en determinadas circunstancias (artículos 15 y 16).

Sobre la revelación del Secreto médico, existen excepciones y exime al médico de guardar el secreto médico en los siguientes casos:

a) Cuando el paciente o su responsable legal autoriza expresamente al médico a revelarlo.

b) Cuando actúa en el desempeño de sus funciones como médico forense a requerimiento de autoridad competente.

c) Cuando se trate de casos de enfermedad notificable.

d) Cuando la salud de la familia y la comunidad se encuentren en riesgo inminente.

e) En caso de menores de edad, los padres, parientes o responsables de los mismos no podrán dar a conocer la información sobre el estado médico del menor salvo para dar cumplimiento a lo establecido en la normativa legal.

f) Cuando la ley disponga expresamente (artículo 17).

4.6.6 CONCILIACIÓN Y ARBITRAJE MÉDICO

Se crea el Instituto Médico de Conciliación y Arbitraje que regula la relación de conflicto médico-paciente ocupándose de sus controversias (artículo 18).

A la fecha el Ministerio de Salud no ha constituido el Instituto Médico de Conciliación y Arbitraje.

4.7 REGLAMENTO DE LA LEY DEL EJERCICIO PROFESIONAL MÉDICO

Mediante Decreto Supremo 28562 de fecha 22 de diciembre de 2005 se aprueba el Reglamento de la Ley del Ejercicio Profesional Médico.

4.7.1 DEFINICIONES OPERATIVAS Y COORDINACIÓN

Se resalta la definición de receta médica que establece el Reglamento de la Ley 3131 por la relación que tiene con el tratamiento de datos sanitarios.

Receta médica constituye el documento legal que avala la prescripción facultativa para la dispensación de medicamentos. Consta de dos partes que deben ser legibles: la prescripción propiamente dicha y las indicaciones de uso.

La prescripción debe registrar el nombre del paciente; el nombre genérico, opcionalmente el nombre comercial, forma farmacéutica, concentración y, cuando corresponda, el código del medicamento; fecha, el nombre del médico, la firma, el número de matrícula profesional, la especialidad –cuando corresponda– y el sello del médico, conforme legislación vigente. Las indicaciones de uso: dosis y frecuencia de horario, deben ser registradas en hoja aparte, considerando que la receta médica será retenida en el establecimiento farmacéutico (artículo 6).

4.7.2 DOCUMENTOS MÉDICOS OFICIALES

El expediente médico está constituido por el conjunto de la historia clínica y los documentos relacionados con el caso que surjan por fuera del proceso asistencial.

La historia clínica es el conjunto de documentos escritos e iconográficos generados durante cada proceso asistencial de la persona atendida.

Para fines de atención, conciliación, arbitraje, proceso judicial u otros, el expediente clínico se organiza de la siguiente manera:

Durante la hospitalización:

— Gráficas de temperatura.

— Órdenes médicas.

— Evolución.

— Informes de laboratorio.

— Informe quirúrgico.

— Informe de anestesia.

— Informe de anatomía patológica.

— Notas de enfermería.

— Hoja de medicamentos.

— Historia y examen físico.

— Epicrisis.

— Informe de ingreso y egreso.

Secuencia de formularios de la historia clínica después del egreso:

— Informe de ingreso y egreso.

— Epicrisis.

— Historia y examen físico.

— Evolución.

— Órdenes médicas.

— Informes de laboratorio.

— Informe de anestesia.

— Informe quirúrgico.

— Informe de anatomía patológica.

— Gráfica de temperatura.

— Medicamentos.

— Notas de enfermería (artículo 12).

4.7.3 DERECHOS Y DEBERES; OBLIGACIÓN DE DIFUNDIR

Es obligatoria la difusión de los derechos y deberes de los pacientes y los derechos y deberes de los médicos en todos los sectores del Sistema Nacional de Salud. Esto debe realizarse en todos los establecimientos e instituciones de salud, en forma pública y visible, al alcance de los pacientes y público en general.

El consentimiento expreso se refiere a la voluntad o decisión del paciente de rechazar el tratamiento u hospitalización indicados por el médico tratante, registrado en la historia clínica y debidamente respaldada por la firma del paciente o de su familiar o responsable legal.

En situaciones donde el paciente no tiene capacidad de decidir sobre su persona, requiere intervención profesional médica y no cuenta con un familiar, pariente o responsable legal, la institución de salud asume la decisión terapéutica siguiendo las normas y protocolos vigentes.

Es obligación del médico registrar en la historia clínica la información brindada al paciente respecto al diagnóstico, tratamiento y pronóstico de la enfermedad; este registro debe ser suscrito por el paciente, familiar, pariente o representante legal (artículo 14).

4.7.4 AUDITORÍA MÉDICA INTERNA, AUDITORÍA MÉDICA EXTERNA Y AUDITORES MÉDICOS ACREDITADOS

La auditoría médica constituye un proceso unitario, educativo, preventivo y, según corresponda, también correctivo. Según el propósito, puede ser interna o externa.

La *auditoría médica interna* constituye un procedimiento de aplicación regular, es técnico, evaluativo, preventivo y correctivo para el aseguramiento y mejoramiento de la calidad en salud, que comprende la evaluación de la estructura, proceso y resultados, conducida por los Comités de Auditoría Médica, bajo supervisión del Departamento o Responsable de Gestión de Calidad y Auditoría Médica institucional.

En caso que el Departamento de Gestión de Calidad, Enseñanza e Investigación, en el proceso rutinario de auditoría interna, encuentre

indicios de mala práctica médica, deberá requerir la realización de una auditoría externa a la máxima autoridad departamental de salud. En el primer nivel de atención (Puestos y Centros de Salud), las auditorías internas serán asimiladas a los procesos de auto-evaluación mensual mediante instrumentos vigentes emitidos por el Ministerio del área de Salud (artículo 16).

La *auditoría médica externa* es un procedimiento técnico, analítico, evaluativo, de carácter preventivo y correctivo que se realiza ante denuncias de mala práctica médica. Se aplica al acto médico y consiste en la verificación del cumplimiento de normas y protocolos vigentes. Se realiza mediante el análisis del expediente clínico.

La Autoridad Departamental de Salud en cumplimiento de la normativa vigente, conforma las Comisiones Departamentales de Auditoría Médica, en un plazo máximo de 48 horas de presentada la solicitud, sin que ello implique erogación de recursos económicos adicionales para el Tesoro General de la Nación (TGN). Si la denuncia de mala práctica médica involucra al sector de la Seguridad Social de corto plazo, la Autoridad Departamental de Salud solicitará la intervención del Instituto Nacional de Seguros de Salud (INASES) para que, en uso de sus atribuciones, realice la auditoría médica externa.

La auditoría médica interna y la auditoría médica externa, en caso de los sectores Privado con fines de lucro y Privado sin fines de lucro, son de competencia de la autoridad de salud departamental (artículo 17).

4.8 CÓDIGO DE ÉTICA Y DEONTOLOGÍA DE ENFERMERÍA

Mediante Resolución Ministerial 0071 de fecha 17 de febrero de 2005 se aprueban los documentos que a continuación se citan y que en anexo forman parte integrante e indivisible de la Resolución:

1. Estatuto orgánico del Colegio de Enfermeras de Bolivia.
2. *Código de Ética y Deontología.*
3. Reglamento del ejercicio de la enfermería.
4. Reglamento de Concurso de Méritos y Examen de Competencias.

5. Reglamento del Tribunal de Honor Nacional.
6. Reglamento de Deberes.
7. Reglamento de Sociedad Científica.
8. Reglamento del Comité nacional Electoral (artículo Único).

El inciso *f)* del artículo 7 (Principios de la Ética) del Capítulo II De los Principios y valores del Código de Ética de Enfermería establece: *f)* «Confidencialidad: salvaguardar la información de carácter personal obtenida durante el ejercicio de su función como enfermera (o) y mantener el carácter de secreto profesional de esta información».

El inciso *b)* del artículo 8 (Valores) del Capítulo II De los Principios y valores del Código de Ética de Enfermería establece: *b)* «Respeto a la persona, familia, grupos y comunidad: Respetar la privacidad, autonomía y de derecho de conocer o no conocer sobre su enfermedad durante el ejercicio de su función como enfermera(o)».

El artículo 10 del Capítulo IV, La enfermera y las personas, deberes de las enfermeras del Código de Ética de Enfermería establece: «…Dar una información suficiente que permita el consentimiento fundamentado y el derecho a elegir o rechazar el tratamiento».

En el ejercicio de la enfermería, el consentimiento del usuario sobre las acciones que debe realizar en busca del bienestar del mismo ha de ser solicitado, con carácter previo a cualquier intervención de enfermería y en caso de incapacidad mental o física, por los familiares.

La enfermera deberá valorar en el enfoque holístico (bio-psicosocial) el estado de salud del usuario antes de informar de su real o potencial estado de salud, considerando que este se encuentre en condiciones de comprender, aceptar y decidir; caso contrario, la información requerida se dirigirá a sus familiares.

El inciso *f)* del artículo 15 (Deberes en el Área Clínica) del Capítulo VII, La enfermera y la profesión, deberes de las enfermeras del Código de Ética de Enfermería establece: *f)* «Coordinará con el equipo de salud para dar información a la familia del paciente».

El inciso *f)* del artículo 16 (Deberes en el Área de la Docencia - Formación de Recursos Humanos) del Capítulo VII, La enfermera y la profesión, deberes de las enfermeras establece: *f)* «Planificará, ejecutará, evaluará los programas de educación dirigidos al paciente y a la comunidad».

El inciso *c)* del artículo 21 (Deberes consigo mismo) del Capítulo VIII, La enfermera y sus colegas, el equipo de salud, el colegio y consigo misma, deberes de las enfermeras establece: *c)* «Mantener el secreto profesional en correspondencia al presente código, que solo será relevado en casos previstos por Ley».

Los artículos 31 y 33 del Capítulo X, Del secreto profesional establecen: Mantendrá en reserva como un secreto profesional todo lo que vea, oiga, descubra o le sea confiado en el ejercicio de la profesión; sólo puede ser revelado en caso de ser requerido por autoridades institucionales o jurídicas (artículo 32). La obligación del secreto profesional se mantiene aún después que haya cesado la prestación de los servicios de enfermería, así como con posterioridad a la muerte del paciente (artículo 33).

Finalmente, el Anexo II, De los derechos del paciente, señala: «El paciente tiene derecho a que quede constancia por escrito de todo su proceso; estas informaciones, y las pruebas realizadas constituyen la historia clínica».

4.9 REGLAMENTO PARA LA ELABORACIÓN, MANEJO Y ARCHIVO DEL EXPEDIENTE MÉDICO O CLÍNICO EN LAS ENTIDADES DE LA SEGURIDAD SOCIAL A CORTO PLAZO

Mediante Resolución Administrativa 158/2005, de fecha 28 de diciembre de 2005, el Instituto Nacional de Seguros de Salud (INASES) aprueba el «Reglamento para la elaboración, manejo y archivo del expediente médico o clínico en las entidades de la Seguridad Social a Corto Plazo».

El presente Reglamento tiene por objeto estandarizar la elaboración, manejo y archivo del expediente Médico o Clínico en las entidades de la Seguridad Social de Corto Plazo y los Seguros Delegados en Bolivia (artículo 1).

El Reglamento considera las siguientes definiciones:

a) *Expediente médico o expediente clínico:* es el conjunto de documentos escritos e iconográficos generados durante cada proceso asistencial de la persona atendida en servicios de consulta externa, emergencia y hospitalización de los Entes Gestores, los cuales refleja-

rán toda la información relativa a su estado de salud o enfermedad. Es un documento técnico, científico, administrativo y legal, utilizado para la evaluación de la calidad de los servicios médicos, odontológicos, enfermería y otros. El expediente médico o clínico está compuesto por: hoja de admisión, historia clínica, exámenes complementarios y auxiliares, evolución y tratamiento, solicitud de interconsultas, consentimiento informado, parte de baja, alta médica, hojas de enfermería, informe de juntas médicas, epicrisis.

b) *Historia Clínica:* es un documento técnico, científico, legal, administrativo y confidencial, en el que se registran los datos en orden cronológico concernientes al proceso salud-enfermedad que se inicia con la filiación y termina con el plan terapéutico. Debe ser elaborada en los servicios de consulta externa, emergencia y hospitalización.

c) *Consentimiento Informado:* es una declaración de voluntad efectuada por el paciente, familiares de primer grado o su representante legal, el cual luego de recibir información suficiente con respecto a su enfermedad y al procedimiento o intervención quirúrgica que se le propone médicamente aconsejable como la más correcta para la solución, mitigación o rehabilitación de su problema de salud, decide dar su conformidad y someterse a tal procedimiento o intervención.

d) *Atención Médica:* conjunto de servicios multidisciplinarios que se proporciona al usuario, con el fin de restaurar, proteger y promover su salud.

e) *Resumen Clínico:* (En casos de interconsultas, referencia o actualización del caso). Es el documento elaborado por el médico tratante, en el cual se registrarán los aspectos relevantes de la atención médica de un paciente, contenidos en el expediente clínico. Deberá contener como mínimo: padecimiento actual, diagnósticos, tratamientos, evolución, pronóstico, estudios de laboratorio y gabinetes.

f) *Médico tratante:* Profesional del área médica acreditado por las instancias legales respectivas, responsable del acto médico desde el inicio de la atención hasta su referencia, alta definitiva o voluntaria.

g) *Acto médico:* Toda intervención profesional del médico, respaldada por protocolos, normas, o información científica basada en la mejor evidencia, con calidad y calidez humana.

h) *Referencia y contrarreferencia:* Es el procedimiento médico administrativo entre unidades operativas de los tres niveles de atención para facilitar el envío, recepción y retorno de pacientes con el propósito de brindar atención médica integral y de calidad.

i) *Interconsulta:* Procedimiento que permite la participación de otro profesional de la salud a fin de clarificar diagnóstico, indicar tratamientos o proporcionar rehabilitación al usuario.

j) *Usuario(a):* Asegurado, beneficiario, derecho habiente o persona particular que solicita atención médica (artículo 2).

El Reglamento del Expediente Médico o Clínico es de observancia y cumplimiento obligatorio en el ámbito de los establecimientos de atención médica de los Entes Gestores de la Seguridad Social de Corto Plazo y Seguros Delegados (artículo 3).

Todo expediente médico o clínico debe cumplir con las siguientes características:

a) Es único por persona para todo el proceso de atención médica.

b) Es acumulativo, porque toda la información de salud generada sobre el usuario durante los procedimientos asistenciales se incorporará en una sola carpeta.

c) Es integrado, por contener toda la documentación de los procesos de salud efectuados en diferentes servicios.

d) Es confidencial, porque la información que contiene no es pública y forma parte del secreto profesional.

e) Contiene información disponible para el personal de salud autorizado, en función al requerimiento o

f) necesidad.

g) Debe ser completo, continuo, legible, sin abreviaturas, sin enmiendas ni tachaduras, ordenado, foliado, conservarse en buen estado y realizado en los formularios diseñados para la respectiva función.

h) Las notas de interconsultas se ajustarán a los principios técnicos y éticos que orientan la práctica médica y a todo lo establecido en el presente reglamento (artículo 4).

El expediente clínico tiene las siguientes funciones:

a) *Función informativa:* El Expediente Clínico permite registrar datos sobre el estado de salud del usuario; para el adecuado seguimiento e información del equipo de salud u otras instancias reconocidas por ley sobre el proceso y la evolución por los que transcurre el paciente.

b) *Función probatoria:* El Expediente Médico o Clínico es el único documento que acredita o exterioriza la existencia de la relación institucional del médico y del paciente, pudiendo constituirse en una prueba para establecer las responsabilidades determinadas por ley.

c) *Función estadística:* Es un elemento base del Sistema de información del establecimiento y la institución para la toma de decisiones gerenciales.

d) *Función evaluadora:* El Expediente Médico o Clínico podrá ser utilizado para evaluar el acto médico, a través de técnicas reconocidas por la norma jurídica vigente.

e) *Función de enseñanza e investigación:* Podrá ser utilizado en los procesos de enseñanza-aprendizaje e investigación (artículo 5).

Bajo el principio básico de respeto a la dignidad humana, el expediente clínico garantiza la confidencialidad de la información relacionada con las prestaciones de salud que se dan a los usuarios protegiendo la privacidad de la misma por medios adecuados que la salvaguarden en los procesos de obtención, utilización, archivo, custodia y trasmisión.

El personal de salud debe considerar la discrecionalidad y confidencialidad del expediente clínico y sólo se rompe el secreto profesional en los casos establecidos en el Capítulo VII artículo 17 de la Ley 3131, de 8 de agosto de 2005 (artículo 11).

El expediente clínico es un documento médico legal de propiedad del establecimiento de salud (hospital, policlínico, clínica o centro de salud) y por consiguiente ningún funcionario podrá retirarlo fuera de la institución o utilizarlo sin la autorización por autoridad respectiva. Solo en caso de requerimiento por autoridad competente podrán emitirse fotocopias autentificadas por la Unidad Jurídica de la entidad y avaladas por el Director del establecimiento de salud. Según Resolución Ministerial 028/97 (artículo 12).

En relación al requerimiento del Expediente Médico o Clínico:

a) El Expediente Clínico deberá ser requerido en la Unidad de Admisión tanto para la primera consulta o consulta subsiguiente, debiendo esta unidad registrar los datos generales y administrativos en el formulario admisión, transfiriendo la ficha a la Unidad de Archivo para la identificación y remisión del Expediente Clínico al consultorio correspondiente.

b) La Responsabilidad para requerir los expedientes clínicos y devolverlos al encargado de Archivo será de la Licenciada o Auxiliar de Enfermería del servicio correspondiente, debiendo registrar estas acciones de acuerdo a la modalidad de cada institución.

c) El tiempo para la devolución de los expedientes clínicos al Archivo deberá estar sujeto a reglamentaciones internas de acuerdo a las particularidades de cada institución (artículo 13).

d) Sobre el archivo del Expediente Médico o Clínico:

e) Los expedientes clínicos deberán ser conservados por un periodo de cinco años en archivo a partir del último acto médico.

f) A partir del sexto año, la institución podrá organizar sus archivos en depósitos, medios magnéticos u otros que la tecnología pueda proporcionar teniendo en cuenta que se debe contar con un resumen de todos sus expedientes clínicos.

g) El área de archivo debe ser un espacio que brinde seguridad a los expedientes con el equipo, mobiliario suficiente y tener la señalización correcta para el manejo por índice alfabético o código de acuerdo al procedimiento que se decida emplear.

h) Debe contarse con un registro único y confiable (listado de expedientes) o con una metodología de archivo de acuerdo con las características de cada entidad gestora, que permita identificar con facilidad la ubicación de los expedientes requeridos al momento necesario.

i) Debe designarse un Responsable del Archivo con formación en el tema y cuyas funciones están establecidas en el manual de funciones y reglamento interno de la entidad (artículo 14).

4.10 LEY PARA LA PREVENCIÓN DEL VIH-SIDA, PROTECCIÓN DE LOS DERECHOS HUMANOS Y ASISTENCIA INTEGRAL MULTIDISCIPLINARIA PARA LAS PERSONAS QUE VIVEN CON EL VIH-SIDA

La Ley 3729 para la prevención del VIH-SIDA, protección de los derechos humanos y asistencia integral multidisciplinaria para las personas que viven con el VIH-SIDA, aprobada en fecha 8 de agosto de 2007, tiene como objeto:

a) Garantizar los derechos y los deberes de las personas que viven con el VIH – SIDA, así como del personal de salud y de la población en general.

b) Establecer políticas y ejecutar programas para la prevención, atención y rehabilitación del VIH-SIDA y la protección de los derechos.

c) Definir las competencias y responsabilidades del Estado, sus instituciones y las personas naturales o jurídicas relacionadas con la problemática del VIH-SIDA.

d) Establecer mecanismos de coordinación interinstitucional e intersectorial, conducentes a la implementación efectiva de las políticas y programas para prevención, asistencia integral multidisciplinaria y rehabilitación de las personas que viven con el VIH-SIDA, a través de campañas de información mediante el uso de medicamentos antirretrovirales y profilácticos, exámenes de laboratorio requeridos, vigilancia epidemiológica e investigación del VIH-SIDA.

La Ley 3729 se enmarca en los siguientes principios:

— Dignidad.

— Igualdad.

— Universalidad.

— Confidencialidad.

— Integralidad.

— Responsabilidad.

De los citados principios sobresalen los relacionados con la protección de datos sanitarios:

— *Dignidad:* toda persona que vive con el VIH-SIDA recibirá un trato digno acorde a su condición de ser humano y no puede ser sometido a discriminación, degradación, marginación o humillación. Goza de los derechos, libertades y garantías reconocidos por la Constitución Política del Estado. Este principio incluye a los familiares de las personas que viven con el VIH-SIDA.

— *Confidencialidad:* la condición clínica de las personas que viven con VIH-SIDA deben sujetarse a normas de confidencialidad establecidas en los códigos de ética, protocolos médicos y epidemiológicos y la Ley (artículo 2).

El Ministerio de Salud, que es la autoridad competente para la aplicación de la Ley 3729, a través del Programa Nacional de ETS/SIDA, debe implementar políticas nacionales orientadas a la educación y promoción de la salud; la prevención, diagnóstico, vigilancia epidemiológica y tratamiento del VIH-SIDA (artículo 4).

Predominan los derechos, garantías y deberes de las personas que viven con VIH-SIDA, relacionados con la protección de datos sanitarios:

— A la vida, la salud y la seguridad.

— A que se respete su privacidad, manteniendo la confidencialidad de su estado serológico y prohibiendo las pruebas obligatorias, siempre que no esté afectando a terceras personas. Excepto en los casos especificados en la misma Ley.

— A la protección contra el despido laboral motivado por su condición de vivir con el VIH-SIDA. Las personas que viven con el VIH-SIDA tienen derecho al trabajo y pueden desempeñar sus labores de acuerdo a su capacidad, no pudiendo considerarse el VIH-SIDA como impedimento para contratar, ni como causal de despido (artículo 5).

El artículo 7 sobre protección de niños y niñas que viven o conviven con VIH-SIDA establece que ningún niño puede ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su entorno social, su domicilio o su correspondencia, ni de ataques ilegales a su honra o reputación a causa de su estado serológico.

Sobre el derecho a la reserva establece que las personas que viven con VIH-SIDA, tienen derecho a la reserva de su identidad y situa-

ción, para ello las autoridades judiciales se encuentran obligadas al resguardo de su identidad, en todas las instancias del proceso, para este efecto se utiliza un código o nomenclatura codificada, salvo petición y consentimiento de la persona afectada.

El personal de salud, que por razones de su trabajo toma conocimiento de la identidad de las personas que viven con el VIH-SIDA, no puede divulgar la identidad de ninguna manera, salvo lo dispuesto en los diferentes protocolos médicos y epidemiológicos.

Las personas que viven con VIH-SIDA no deben ser objeto de publicaciones de prensa escrita ni televisiva[45], sin su consentimiento expreso (artículo 9).

El artículo 19, sobre pruebas para el diagnóstico de VIH-SIDA, establece que ninguna persona será sometida a pruebas obligatorias para el diagnóstico de VIH-SIDA, salvo en los casos que se establecen a continuación, sujetos a normas de atención:

a) Para efectos de donar sangre, hemoderivados, leche materna, semen, órganos o tejidos.

b) Para la emisión del carnet sanitario a personas de ambos sexos que se dedican al comercio sexual.

c) Enjuiciamiento penal por transmisión a personas, en estos casos la prueba se realizará con orden emitida por juez competente.

d) Para fines de vigilancia epidemiológica e investigación en la población que enfrenta un riesgo potencial e inminente de transmisión.

e) En pacientes con insuficiencia renal crónica, antes de entrar a los programas de hemodiálisis.

---

[45] Un caso emblemático es el linchamiento mediático que sufrió el Magistrado del Tribunal Constitucional Plurinacional, Gualberto Cusi por las declaraciones del 22 de diciembre de 2014 del ex Ministro de Salud, Juan Carlos Calvimontes, quién declaró en conferencia de prensa que «el magistrado padece una enfermedad terminal y tuberculosis». Viernes 26 de diciembre de 2014 Calvimontes dijo que quiso precautelar la salud de la población, porque Cusi «es doblemente peligroso para la sociedad» por no tomar sus medicamentos. Diario Página Siete (2014): «El ministro busca que enfermos de VIH-Sida sean estigmatizados» [en línea]: http://www.paginasiete.bo/sociedad/2014/12/27/ministro-busca-enfermos-vih-sida-sean-estigmatizados-42383.html [Consulta: 19/01/2014].

f) En pacientes programados para intervenciones quirúrgicas y aquellos que vayan a ser sometidos a métodos de diagnóstico invasivo.

g) A los que presenten una o varias ETS y a los que manifiestan alguna conducta de riesgo.

h) En los niños nacidos de madres VIH (+).

Las pruebas para el diagnóstico del VIH-SIDA deben realizarse acompañadas con pre y post consejería, con el consentimiento informado de la persona o de su representante legal, a no ser que se encuentre dentro de las excepciones previstas por la presente ley.

Los resultados de las pruebas de diagnóstico del VIH-SIDA serán confidenciales y la identidad guardada bajo códigos, para lo cual todo centro médico o laboratorio público o privado, debidamente acreditado, que detecte un caso de VIH-SIDA debe notificar este hecho de manera confidencial a las autoridades del Programa Nacional de ETS/VIH-SIDA del Ministerio de Salud y Deportes para lo cual se habilita un registro codificado de casos detectados y su evolución (artículo 20).

4.11 REGLAMENTO DE LA LEY 3729 PARA LA PREVENCIÓN DEL VIH – SIDA

El Decreto Supremo 0451, de fecha 17 de marzo de 2010, reglamenta las disposiciones contenidas en la Ley 3729, de fecha 8 de agosto de 2007, para la prevención del VIH[46] – SIDA[47].

Las disposiciones contenidas en el Decreto Supremo son de cumplimiento obligatorio en todo el Sistema Nacional de Salud que comprende al Sistema Público, Seguro Social de corto plazo, instituciones públicas y privadas que trabajan en el área de salud con y sin fines de lucro, ONG, profesionales en salud independientes y perso-

---

46 VIH: Virus de Inmunodeficiencia Humana, causante de la enfermedad denominada SIDA (D.S. N.º 041).

47 SIDA- Síndrome de Inmuno Deficiencia: Conjunto de síntomas y signos generados por el compromiso del sistema inmunitario de un individuo como consecuencia de la infección por el VIH. Estadio final de la infección por el virus (D.S. N.º 041).

nas naturales y jurídicas, nacionales y extranjeras, sin excepción alguna (artículo 2).

El Programa Nacional ITS/VIH/SIDA dependiente de la Unidad de Epidemiología de la Dirección General de Servicios de salud del Ministerio de Salud y Deportes, como instancia operativa en el tema de VIH – SIDA, propone como objetivo general en el Plan Estratégico Multisectorial. Reducir la concurrencia de nuevas infecciones por ITS y VIH, la morbilidad y mortalidad de las personas que viven con VIH – SIDA (artículo 7).

Todo centro de atención médica, público o privado de la seguridad social, ONG, militar, policial, de institución religiosa, legalmente autorizado, que detecte un caso de VIH – SIDA debe noticiarlo al Programa Nacional ITS/VIH/SIDA, aun en caso de fallecimiento del paciente, guardando absoluta confidencialidad sobre los resultados y la identidad del mismo, a cuyo efecto los datos personales deben ser codificados. La información sobre detección de nuevos casos posteriormente será remitida por el Programa Nacional ITS/VIH/SIDA, al Servicio Nacional de Información en Salud – SNIS para fines de información estadística (artículo 28).

Salvo las excepciones establecidas en el artículo 19 de la Ley 3729, ninguna persona será sometida a pruebas obligatorias de VIH - SIDA. Las pruebas se realizarán conforme a normas y protocolos establecidos por el Ministerio de Salud y Deportes (artículo 31).

El Programa Nacional ITS/VIH/SIDA normará el servicio de pre[48] y post consejería[49] para la prueba voluntaria de diagnóstico (artículo 33).

El carácter confidencial de los resultados de las pruebas de diagnóstico de VIH tiene las siguientes excepciones:

a) Podrán ser solicitados por el Ministerio Público o Poder Judicial, mediante requerimiento u orden judicial, siempre que las cir-

---

48 Pre – consejería: Orientación a cargo de un profesional capacitado a una persona con carácter previo a una prueba de diagnóstico de VIH (D.S. N.º 0451).

49 Post – consejería: Orientación profesional a una persona que se haya sometido a una prueba de diagnóstico de VIH (D.S. N.º 0451).

cunstancias lo justifiquen y para fines de investigación delictiva o en procesos en materia familiar.

b) Podrá informarse a otro profesional en salud cuando sea necesario para el seguimiento, tratamiento y control de la persona infectada (artículo 34).

En el marco del derecho a la confidencialidad, el expediente clínico de toda PVVS[50] deberá ser objeto de cuidadoso manejo, de tal manera que se impida el acceso a la información confidencial contenida en el mismo a personas no autorizadas o que no estén involucradas en la atención al paciente (artículo 42).

Los establecimientos de los tres (3) niveles de atención en salud de todos los componentes del Sistema Nacional de Salud están obligados a prestar en forma inmediata los servicios de atención a las personas con VIH - SIDA, no pudiendo negar dicha atención bajo ninguna circunstancia o causal alguna (artículo, 46).

En el ámbito educativo ninguna entidad educativa, de ningún nivel de formación profesional, técnica, civil, militar, policial, pública o privada, podrá discriminar a un postulante o a un estudiante por su condición de PVVS (artículo 49).

Ningún centro educativo, de ningún nivel, público o privado podrá solicitar pruebas[51] ni dictámenes médicos sobre VIH, como requisito de ingreso o permanencia en el establecimiento. Asimismo, ningún estudiante será discriminado, excluido o expulsado por ser PVVS (artículo 52).

En el ámbito laboral, las personas que viven con VIH tienen los mismos derechos que las otras personas de postular a un puesto de trabajo en cualquier centro laboral público o privado, de acuerdo a sus aptitudes personales y formación, sin que su condición clínica sea factor determinante para su exclusión (artículo 54).

---

50 PVVS: Persona viviendo con VIH – SIDA.

51 Prueba de diagnóstico de la infección del VIH – Sida: Examen serológico para determinar infección por el VIH en un individuo. Puede ser presuntiva, cuando su resultado en caso de ser reactivo, requiere otro procedimiento laboratorial de confirmación (examen serológico de alta especificidad) (D.S. N.º 0451).

Las PVVS no pueden ser rechazadas ni discriminadas por su condición clínica a tiempo de ser contratadas para un puesto de trabajo (artículo 55).

Ninguna persona con VIH puede ser retirada de su fuente laboral por su condición serológica, salvo las causales previstas en el artículo 16[52] de la Ley General del Trabajo, para los trabajadores del área privada, y el artículo 32[53] de las Normas Básicas del Sistema de Administración de Personal, en el caso de los servidores públicos (artículo 56).

Está prohibida toda forma de trato discriminatorio relacionado con el VIH en el ámbito laboral contra cualquier trabajador (artículo 57).

El acceso eventual a datos personales de un trabajador que vive con VIH-SIDA debe sujetarse a normas de confidencialidad establecidas por ley (artículo 58).

Las infracciones a la Ley 3729 y al presente Reglamento, cometidas por las instituciones prestadoras de servicios de salud y/o el personal de salud, dará lugar a la imposición de sanciones administrativas, civiles o penales correspondientes, de acuerdo a reglamentación específica emitida por el Ministerio de Salud y Deportes (artículo 66).

4.12 NORMA TÉCNICA PARA EL MANEJO DEL EXPEDIENTE CLÍNICO

El Ministro de Salud y Deportes[54] aprueba, en fecha 28 de febrero de 2008, la Resolución Ministerial 0090 en la cual pone en vigencia la Norma Técnica del Expediente Clínico que tiene como objetivo

---

52 Artículo 16: «No habrá lugar a desahucio ni indemnización cuando exista una de las siguientes causales: a) perjuicio material causado con intención en los instrumentos de trabajo, b) Revelación de secretos industriales, c) Omisiones o imprudencias que afecten a la seguridad o higiene industrial, d) Inasistencia injustificada de más de seis días continuos, e) Incumplimiento total o parcial del convenio; f) retiro voluntario del trabajador; g) Robo o hurto por el trabajador. Ley General del Trabajo Decreto Ley de 24 de mayo de 1939, elevado a Ley de la República el 8 de diciembre de 1942.

53 Artículo 32.

54 La denominación de Ministerio de Salud y Deportes cambia a Ministerio de Salud.

establecer la norma y metodología con fundamentos científicos, tecnológicos, administrativos, éticos y jurídicos, para la elaboración, integración, ordenamiento, uso y archivo del Expediente Clínico, en aras al mejoramiento de la calidad en todo el Sistema Nacional de Salud (artículo 2).

El Sistema Nacional de Salud (SNS), encabezado y regulado por el Ministerio de Salud, es el conjunto coordinado de instituciones y establecimientos que prestan servicios de salud[55] a la población, en los sectores público, seguridad social de corto plazo, privado no lucrativo y privado lucrativo, incorporándose además la medicina tradicional y la medicina alternativa.

A partir de la formulación de este documento el Ministerio de Salud, pretende que su manejo habitual sea cuidadoso en todos los servicios de salud, siendo obligación del Ministerio de Salud establecer una norma para corregir esta situación, proteger la salud de la población y promover la excelencia en la elaboración y utilización del Expediente Clínico, que es uno de los indicadores más confiables para constatar la calidad en la prestación de los servicios de salud.

El Expediente Clínico (EC) es el conjunto de documentos escritos e iconográficos evaluables que constituyen el *historial clínico* de una persona que ha recibido o recibe atención en un establecimiento de salud. Su manejo debe ser escrupuloso porque en él se encuentran todos los datos que permiten encarar de la mejor manera el estado de salud-enfermedad del paciente y su respectivo tratamiento (artículo 5.1).

La Norma Técnica tiene como objetivos específicos:

— Establecer la elaboración obligatoria del EC con sus respectivos componentes documentales, en todos los servicios de salud.

— Estandarizar el manejo habitual del EC.

— Sistematizar la conservación y archivo del EC.

— Promover la cultura de la calidad en el Sistema Nacional de Salud, a través del manejo adecuado del EC (artículo 3).

---

[55] Institución Prestadora de Servicios de Salud: Es todo aquel organismo, institución o establecimiento, ya sea del sector público estatal, municipal, seguridad social o sector privado con y sin fines de lucro, que habilitado y autorizado de acuerdo al marco legal vigente, ofrece y brinda servicios de salud a la población.

La Norma Técnica define al consentimiento informado como «la potestad que tiene el paciente de aceptar libremente y sin presiones, que por necesidad diagnóstica o terapéutica, se practique en su propio cuerpo algún procedimiento clínico, laboratorial, imagenológico o instrumental, previa explicación clara de quien lo tenga que practicar, con el fin de que el paciente sepa y comprenda cómo será realizado y cuáles son sus beneficios y eventuales riesgos o perjuicios, a más de obtener repuesta a sus preguntas e inquietudes» (artículo 5.4).

Para lograr que el Expediente Clínico (EC), sea un instrumento de interpretación y uso confiable, debe cumplir las siguientes condiciones básicas:

— *Veracidad:* Consiste en la descripción veraz de todo lo referente al estado de salud enfermedad del paciente y los procedimientos realizados para su diagnóstico, tratamiento y/o rehabilitación.

— *Carácter científico:* Consiste en el apego a la *lex artis medicae*.

— *Integridad:* Consiste en la presencia de datos clínicos suficientes sobre el estado de salud-enfermedad del paciente, complementados por métodos auxiliares de diagnóstico y tratamiento, junto a notas de evolución, tratamientos, consentimiento informado y documentos administrativos destacables de los procesos cumplidos durante la atención del paciente, refrendados todos con nombre, firma y sello o identificación escrita de las personas responsables.

— *Sujeción a la norma:* Consiste en el estricto cumplimiento de la norma existente para la elaboración y manejo del EC, así como de la utilización de formularios u otros documentos expresamente diseñados para tales propósitos.

— *Secuencialidad:* Está referida a los registros de atención, consignados en secuencia cronológica.

— *Disponibilidad:* Es el acceso al EC en el momento en que se lo necesite, con las limitaciones que impone la norma.

— *Exclusividad:* Se refiere a la existencia de un EC exclusivo y específico para cada paciente en el establecimiento donde es atendido. Puede tener carácter acumulativo, dependiendo de las veces que el paciente acuda a la consulta o sea internado, ya sea por causas de una misma enfermedad u otras.

— *Unicidad:* Esta referida a la existencia de formatos únicos y generales de EC para todo el Sistema de Salud, adecuados a los respectivos niveles de atención y las características propias de cada una de las especialidades existentes.

— *Codificación:* Se refiere a la asignación de un número de identificación al EC, que debe ser único y el mismo para todos los documentos que lo constituyen y con el que figure en el archivo estadístico (artículo 6).

La Norma Técnica del Expediente Clínico define a la historia clínica como: «el documento central del EC que a más de señalar los datos generales del paciente y sus antecedentes personales, familiares, no patológicos, patológicos y gineco-obstétricos en el caso de la mujer; describe las condiciones actuales de su estado de salud - enfermedad, investigadas y recogidas a través de la anamnesis o interrogatorio y el examen físico general y especial. Concluye estableciendo el diagnóstico presuntivo, diagnósticos diferenciales y una propuesta básica de conducta y tratamiento» (artículo, 12.4).

Ni ética ni jurídicamente es admisible impedir que el paciente tenga acceso a su Expediente Clínico las veces que lo requiera, ya sea por solicitud directa o por intermedio de su tutor jurídicamente responsable si se encuentra internado, o a través de solicitud notariada dirigida al director del establecimiento si no lo está. En tales casos, el director accederá a la solicitud, disponiendo la entrega –según posibilidades de la institución– ya sea de una copia magnética o de una copia fotostática del EC del paciente, debidamente firmada y sellada en cada uno de sus folios, cotejados con los originales en presencia del paciente o su representante legal. Todo este procedimiento constará en el levantamiento de un acta de entrega, que será firmada por el paciente o su representante legal y por el director del establecimiento, en copias para ambas partes (artículo 23).

La petición de Informe Médico puede estar vinculada a motivos de interés particular como de origen legal o público. Por tanto, el valor de prueba y de garantía que el ordenamiento jurídico y la sociedad confieren a los informes médicos, obliga a extremar el rigor de su contenido, evitando incluir en ellos términos ambiguos o informaciones insuficientes o excesivas que pueden confundir al destinatario. Entre los informes médicos se encuentra la «epicrisis» que es el documento emitido por el médico responsable al finalizar cada proceso asistencial de un paciente en un centro sanitario, y en el que se inclu-

ye, además de un breve resumen de la historia clínica, los datos más relevantes de la actividad asistencial prestada, y las correspondientes recomendaciones terapéuticas (artículo 12.9).

4.13 CÓDIGO DE ÉTICA Y DEONTOLOGÍA MÉDICA

El Código de Ética y Deontología Médica es el conjunto de normas que atañen al médico en su relación con el paciente, la sociedad y su entorno, en el ejercicio de su profesión (artículo 1.º).

En relación a los derechos del paciente, el médico debe actuar siempre en función del interés del paciente, brindándole todos los cuidados necesarios y fundados en conocimientos científicos consagrados, solicitando la colaboración de otros médicos cuando el caso lo requiera (artículo 110).

El paciente tiene derecho a recibir información comprensible sobre su estado, condición y grado de enfermedad para otorgar su consentimiento para la realización de cualquier procedimiento o tratamiento médico. Si no estuviera en condiciones de expresar su voluntad, se requerirá la autorización a sus familiares, salvo urgencias o imposibilidades conforme lo previsto en los artículos 22[56], 23[57], 24[58] y 25[59] (artículo 112).

---

[56] Artículo 22 (Acto Médico en casos especiales).- «En caso de inconsciencia, incapacidad mental o legal del paciente, el médico debe requerir el consentimiento informado y escrito de sus familiares o apoderados en presencia de testigos. En situaciones de urgencia y ausencia de responsables, debe contar, en lo posible, con la opinión autorizada y aquiescencia escrita de uno o dos médicos llamados en consulta».

[57] Artículo 23 (Acto médico en casos de emergencia).- «Si en un caso de emergencia no fuera posible obtener el consentimiento informado, siempre y cuando el criterio clínico aconsejara un tratamiento médico o quirúrgico inmediato, el médico quedará facultado para realizar el tratamiento, sin necesidad de autorización alguna».

[58] Artículo 24 (De la competencia del médico en casos de emergencia). «Independientemente de su función o especialidad, el médico debe prestar auxilio inmediato al enfermo en peligro. El acto médico en este caso, no implica responsabilidad por resultados no deseados».

[59] Artículo 25 (El acto médico en menores de edad). «No se realizará acto médico alguno a pacientes menores de edad sin previo y pleno consentimiento informado y escrito de los padres o tutores; a menos que la vida o que el futuro del paciente exija intervención de urgencia».

El paciente tiene derecho a:

a) Rechazar procedimientos y tratamientos propuestos y a ser informado de lo que implica su decisión.

b) Rechazar ser sujeto de protocolos terapéuticos de investigación sin su consentimiento (artículo 113).

El paciente tiene derecho a exigir que la información concerniente a su estado, tratamientos u otros, no sea revelada a terceros (artículo 114).

El paciente tiene derecho a exigir que las presentaciones de su caso, discusiones, consultas, exploraciones y tratamientos sean conducidos con la discreción, respeto al pudor y a la intimidad que merece (artículo 115).

El Capítulo XVIII del Código de Ética y deontología médica establece que, sobre los documentos médicos, el expediente clínico constituye un conjunto de documentos escritos de orden médico legal, de propiedad del médico en el ejercicio privado y de las instituciones públicas o particulares en el ejercicio institucional. Debe contener toda la información sobre la apreciación y evolución clínicas, los procedimientos médicos efectuados y los exámenes complementarios realizados (artículo 128).

La historia clínica elaborada en forma clara y legible debe llevar siempre el sello y la firma del médico tratante, quien es el responsable de su contenido (artículo 129).

El expediente clínico, por constituir un documento médico legal, es único y su contenido no puede ser modificado o adulterado en beneficio del médico, terceras personas, o perjuicio del paciente (artículo 130).

Se considera abuso de la información falta a la ética, el médico que usa la información contenida en una historia clínica elaborada por otro médico sin su consentimiento, para fines ajenos a la atención del paciente (artículo 131).

En el ámbito privado, el médico tiene la obligación de proporcionar al paciente, cuando solicita, la información contenida en su expediente clínico o facilitar el mismo a otro colega (artículo 132).

En el ámbito Institucional, corresponde a la institución empleadora la responsabilidad de otorgar copias del expediente clínico, según Resolución Ministerial 028/97 (artículo 133).

El médico y, en su caso, la institución para la que trabaja están obligados a conservar el expediente clínico completo, durante cinco años a partir de la última atención (artículo 134).

Cuando un médico cesa en su trabajo privado, su archivo de expedientes clínicos podrá ser transferido al colega que le suceda, salvo que el paciente manifieste su voluntad en contra (artículo 136).

El Médico que quiera conocer el contenido de una historia clínica en el ámbito privado o Institucional debe hacer el requerimiento al profesional médico o la Institución responsable del paciente (artículo 137).

4.14 OBTENCIÓN DEL CONSENTIMIENTO INFORMADO

El consentimiento informado se enmarca, primero, en el derecho que tienen los pacientes y sus familiares de recibir información y, segundo, en el principio ético denominado autonomía; es decir, la capacidad del paciente de aceptar o rechazar la propuesta de diagnóstico y/o tratamiento del proveedor de salud, a partir de información oportuna, clara y verdadera.

En consecuencia, proporcionar información es tanto una obligación moral como legal del proveedor de salud, porque además la Ley 3131 del Ejercicio Profesional Médico así lo establece para los médicos. Para el resto de proveedores involucrados en procedimientos diagnósticos y/o terapéuticos de riesgo, la obligatoriedad emana de lo que está establecido en el documento normativo «Obtención del Consentimiento Informado».

La historia del consentimiento informado se remonta a 1957, cuando fue empleado como recurso judicial en California. Hoy, 58 años después, constituye un derecho de los pacientes y un deber de los médicos y otros profesionales de salud.

En Bolivia, la obligación de informar está contemplada e impuesta mediante la Ley 3131 del Ejercicio Profesional Médico de fecha 08 de agosto de 2005 y de su Decreto Supremo Reglamentario 28562 de fecha 22 de diciembre de 2005.

El consentimiento informado tiene que ver con el proceso de recibir información suficiente y clara sobre un determinado procedimiento terapéutico o diagnóstico, entender esa información y, como consecuencia, tomar una decisión libre de aceptación o rechazo.

El formulario llenado de consentimiento informado, o en su ausencia, lo que queda registrado en la historia clínica, constituye el soporte documental que verifica que el paciente (o su representante legal) ha recibido y entendido la información facilitada por el médico, el odontólogo, el profesional o el técnico encargado del procedimiento diagnóstico o terapéutico.

La no obtención del consentimiento informado puede significar una lesión a los derechos personalísimos del paciente, pero no es la causa del daño, así como el consentimiento informado no legítima la mala praxis. La obtención del consentimiento informado no es un simple trámite expresado en un formulario, sino un «documento médico-legal».

El consentimiento informado constituye una prueba de la comprensión de la situación por el paciente y/o familiares, así como la decisión de elegir un mal menor para prevenir o evitar uno mayor que puede ser el agravamiento de la salud, o incluso la muerte.

Además de ser obligatorio, el formulario llenado y firmado es conveniente para deslindar responsabilidades de sucesos previsibles. Es una oportunidad para que el paciente y familiares formulen preguntas sobre la situación, que podría no darse si resulta omitido el proceso de información. El proceso permite una mejor preparación del paciente, tanto emocional como clínica.

Si el formulario es insuficiente o no existe un formato específico para algún caso en particular, hay que registrar en la historia clínica todo lo que corresponde o falte, así como las rúbricas o huellas dactilares de los actores y testigos.

Así como en las urgencias se diluye la obtención del consentimiento informado e incluso puede no ser posible obtenerlo por tiempo y/o ausencia de allegados, es imprescindible en las cirugías programadas, o cuando se trata de procedimientos médicos o quirúrgicos que pueden ser cancelados o postergados sin que sea afectada de forma inmediata la salud del paciente.

Debido a que el formato de consentimiento informado tiene que ser leído por el paciente y/o familiares, tanto la parte impresa como la

que es realizada a mano, no debe contener abreviaciones, siglas, términos científicos (excepto los muy conocidos).

La Ley 3131 del Ejercicio Profesional Médico establece que el Consentimiento Informado constituye un documento médico oficial (artículo 10 del Capítulo IV). La mencionada ley en el inciso j) del artículo 12 dispone que el llenado de este instrumento sea responsabilidad del médico. En consecuencia, su incumplimiento puede traer aparejados perjuicios profesionales y patrimoniales en casos de litigio.

El consentimiento informado se basa en el derecho que tienen los pacientes de poder conocer todo aquello que deseen con el fin de tomar libremente la decisión de continuar adelante o no con la propuesta diagnóstica o terapéutica del médico. Este derecho está amparado por la Ley 3131 [inciso *e)* del artículo 13] además, le confiere la facultad de «reclamar y denunciar si considera que sus derechos humanos han sido vulnerados durante la atención médica» [inciso *g)* del artículo 13].

Finalmente, el Glosario del Decreto Supremo 0451 de fecha 17 de marzo de 2010 que reglamenta las disposiciones contenidas en la Ley 3729 de fecha 8 de agosto de 2007 para la prevención del VIH[60] – SIDA establece sobre el Consentimiento Informado «asentimiento dado por una persona para someterse a una prueba de detección de VIH en su organismo, luego de haber recibido información a cargo de un profesional. Este consentimiento debe ser expresado por escrito en un formulario o ficha elaborado al efecto».

Tabla 5. Consentimiento Informado

Consentimiento informado en la legislación boliviana		
Ley 3131 del Ejercicio Profesional Médico de fecha 8 de agosto de 2005.	Artículo 10 (Documentos Médicos oficiales)	Bajo el resguardo y custodia del establecimiento de salud son de uso exclusivo del médico, siendo los siguientes: c) Consentimiento Informado.

[60] VIH: Virus de Inmunodeficiencia Humana, causante de la enfermedad denominada SIDA (D.S. N.º 041).

Decreto Supremo 28562 que reglamenta la Ley 3131 de fecha 22 de diciembre de 2005	Artículo 14 (Difusión)	En situaciones donde el paciente no tiene capacidad de decidir sobre su persona, requiere intervención profesional médica y no cuenta con un familiar, pariente o responsable legal, la institución de salud asume la decisión terapéutica siguiendo las normas y protocolos vigentes. Es obligación del médico registrar en la historia clínica, la información brindada al paciente respecto al diagnóstico, tratamiento y pronóstico de la enfermedad; este registro debe ser suscrito por el paciente, familiar, pariente o representante legal.
Resolución Ministerial 0071 que aprueba el Código de Ética y Deontología de Enfermería de fecha 17 de febrero de 2005		En el ejercicio de la enfermería el consentimiento del usuario sobre las acciones que debe realizar en busca del bienestar del mismo, ha de ser solicitado con carácter previo a cualquier intervención de enfermería y en caso de incapacidad mental o física el consentimiento lo conseguirá de los familiares.
Resolución Administrativa 158/2005 Reglamento para la elaboración, manejo y archivo del expediente médico o clínico en las entidades de la Seguridad Social a Corto Plazo de fecha 28 de diciembre de 2005	Artículo 2 (Definiciones)	Es una declaración de voluntad efectuada por el paciente, familiares de primer grado o su representante legal, el cual luego de recibir información suficiente con respecto a su enfermedad y al procedimiento o intervención quirúrgica que se le propone médicamente aconsejable como la más correcta para la solución, mitigación o rehabilitación de su problema de salud, decide dar su conformidad y someterse a tal procedimiento o intervención.

Resolución Ministerial 0090 Norma Técnica para el Expediente Clínico de fecha 28 de febrero de 2008	Artículo 5. Definiciones Artículo 5.4. Consentimiento informado	La potestad que tiene el paciente de aceptar libremente y sin presiones que, por necesidad diagnóstica o terapéutica, se practique en su propio cuerpo algún procedimiento clínico, laboratorial, imagenológico o instrumental, previa explicación clara de quien lo tenga que practicar, con el fin de que el paciente sepa y comprenda cómo será realizado y cuáles son sus beneficios y eventuales riesgos o perjuicios, a más de obtener repuesta a sus preguntas e inquietudes».
Resolución Ministerial 0090 Obtención de Consentimiento Informado de fecha 28 de febrero de 2008		El consentimiento informado tiene que ver con el proceso de recibir información suficiente y clara sobre un determinado procedimiento terapéutico o diagnóstico, entender esa información y, como consecuencia, tomar una decisión libre de aceptación o rechazo.
Código de Ética y Deontología Médica	Artículo 112 (Autorizaciones para procedimientos o tratamientos)	El paciente tiene derecho a recibir información comprensible sobre su estado, condición y grado de enfermedad para otorgar su consentimiento para la realización de cualquier procedimiento o tratamiento médico. Si no estuviera en condiciones de expresar su voluntad, se requerirá la autorización a sus familiares, salvo urgencias o imposibilidades conforme lo previsto en los artículos 22 (Acto médico en casis especiales), 23 (Acto médico en casos de emergencia), 24 (De la competencia del médico en casos de emergencia) y 25 (Acto médico en menores de edad)

Decreto Supremo 0451 que reglamenta la Ley 3729 para la prevención del VIH – SIDA de fecha 17 de marzo de 2010	Glosario del Decreto Supremo 0451	Asentimiento dado por una persona para someterse a una prueba de detección de VIH en su organismo, luego de haber recibido información a cargo de un profesional. Este consentimiento debe ser expresado por escrito en un formulario o ficha elaborado al efecto.

Fuente de elaboración: Propia en base a la legislación boliviana vigente.

4.15 MANUAL DE AUDITORÍA Y NORMA TÉCNICA

El Manual de Auditoría y Norma Técnica ha sido aprobado por Resolución Ministerial 0090/2008 de fecha 26 de febrero de 2008.

La auditoría interna, concebida como el mejor instrumento de autoevaluación, está relacionada con la Norma de Evaluación y Acreditación de Establecimientos de Salud, pudiendo adelantarse a los resultados buenos o malos de una evaluación externa, porque permite a los propios funcionarios de un determinado establecimiento hacer una valoración directa, muy precisa y permanente de su propia institución, ya sea para potencializar fortalezas o corregir errores y defectos con la oportunidad debida.

Las finalidades de la auditoría en salud son múltiples, pudiendo mencionarse la evaluación técnico-administrativa-financiera de una determinada organización sanitaria, la ejecución de una política, plan o programa, el funcionamiento de los servicios, la atención directa del paciente por el personal en salud y el acto médico propiamente dicho. La auditoría en cualquiera de sus formas se realizará indefectiblemente contrastando las situaciones analizadas con las leyes, principios, reglas, normas, protocolos, procedimientos y fichas técnicas que estuvieran vigentes en Bolivia. En ausencia de estos instrumentos normativos, se acudirá a normas supletorias a las normas vigentes en países extranjeros reconocidas por la comunidad internacional (OPS/OMS), o la ex-artis basada en evidencia científica y reconocida por las Sociedades Científicas pertenecientes a los colegios profesionales en salud.

La Norma Técnica establece el ámbito de aplicación a instituciones, establecimientos, dependencias y servicios del Sistema Nacional

de Salud (SNS) conformado por los sectores Público, de la Seguridad Social y Privado con y sin fines de lucro, bajo el rol rector del Ministerio de Salud y Deportes (artículo 3).

Se establecen los siguientes tipos de auditoría en salud:

— Auditoría Programática.

— Auditoría de Servicio.

— Auditoría Médica.

Algunas definiciones de interés de la Norma Técnica son:

— *Auditoría en Salud*: Es un procedimiento de evaluación permanente de la calidad de gestión y asistencia de todos los servicios del sector salud, con el fin de detectar su funcionamiento real, estableciendo correctivos y/o estímulos para su mejoramiento (artículo 4.1).

— *Acto Médico*: Es toda atención profesional del médico, respaldada por protocolos y normativa vigente con calidad y calidez humana.

— *Atención en Salud*: Es toda acción que, respaldada por normas y protocolos, realiza el personal que se desempeña en los establecimientos de salud (artículo 4.12).

— *Expediente Clínico*: Es el conjunto de documentos escritos e iconográficos evaluables que constituyen el Historial Clínico de una persona que ha recibido o recibe atención en un establecimiento de salud (artículo 4.19).

— *Peritaje*: Es el procedimiento de análisis y valoración técnico-profesional de un determinado procedimiento o acto médico, realizado por un recurso humano denominado perito, con formación específica y vasta experiencia en el área o especialidad donde se encuentra incluido el procedimiento o acto que se perita (artículo 4.28).

Dependiendo de cuál sea su finalidad, la auditoría en salud toma en consideración uno o más de los siguientes referentes generales que pueden formar parte de la materia de análisis:

«1. Documentación pertinente, ejemplo: Expediente Clínico (EC) para el caso de auditoría médica…» (artículo 5).

El análisis pormenorizado y cronológico del expediente clínico comprenderá a los siguientes elementos:

1. Papeletas de internación.
2. Gráficas de registro de signos vitales.
3. Historia Clínica.
4. Consentimiento informado.
5. Órdenes Médicas.
6. Notas de evolución e interconsultas e informes de Junta Médica.
7. Informes de exámenes de laboratorio y gabinete.
8. Informes de anatomía patológica.
9. Elementos quirúrgicos:

a) Nota quirúrgica.

b) Protocolo quirúrgico.

c) Nota posquirúrgica.

10. Elementos de anestesia:

a) Nota preanestésica.

b) Protocolo del procedimiento anestésico –Hoja de registro anestésico.

c) Nota de recuperación posanestésica.

11. Elementos de enfermería:

a) Notas de tratamiento y medicamentos administrados, con sello, fecha y firma.

b) Hoja de evolución de enfermería con firma, sello, fecha y hora.

c) Kardex de enfermería con identificación de la profesional de enfermería.

d) Epicrisis.

e) Documentos administrativos de ingreso, egreso, referencia y contrarreferencia, alta solicitada, transferencia, fallecimiento y otros.

12. Adicionales: protocolo de autopsia, copia del certificado de defunción, informes de auditoría médica Interna especial o inducida,

ficha social, fichas de programas específicos (tuberculosis, salud sexual y reproductiva, quimioterapia, AIEPI, desnutrición y otros), Historia Clínica Perinatal, certificado médico, recetas y otros (artículo 26).

En relación con la obtención y custodia del Expediente Clínico la Comisión Departamental de Auditoría Médica (CDAME)[61] acudirá al establecimiento de salud de donde procede el caso que motivó la solicitud de la Auditoría Médica y con una credencial específica conferida por el Director del Servicio Departamental de Salud (SEDES) obtendrá, a través del Director del establecimiento, el expediente clínico completo y original del paciente correspondiente al caso para su custodia en el SEDES, en tanto dure todo el proceso de auditoría hasta su finalización, con la previsión de dejar en el establecimiento una copia fotostática del expediente clínico, hasta la devolución del original (artículo 54). Como constancia de la entrega y recepción del Expediente Clínico se llena el acta correspondiente del Formulario 1 con copias debidamente firmadas, tanto para el Director del establecimiento como para la Comisión Departamental de Auditoría Médica (artículo 55).

---

[61] Comisión Departamental de Auditoría Médica.-«Es la comisión autónoma externa conformada por auditores acreditados que de acuerdo a procedimiento convoca la Unidad de Calidad del SEDES para la realización de la AME, o de darse el caso, auditorías programáticas o de servicio» (artículo 4.24).

PARTE III

DESARROLLO DE LA INVESTIGACIÓN

CAPÍTULO V
LA HISTORIA CLÍNICA

5.1 HISTORIA CLÍNICA

La insuficiencia normativa de la Ley General de Sanidad de España, para dar respuesta a todas las cuestiones que se plantean en relación con la historia clínica, ha provocado proliferación de las normas autonómicas reguladoras de esta materia, que han venido construyendo sistemas de información y documentación clínica no homogéneos.

Con la promulgación de la Ley Básica de Autonomía de los Pacientes (en adelante Ley 41/2002) existe ya una normativa básica, que puede ser objeto de ejecución y desarrollo por las Comunidades Autónomas que garantice unos derechos básicos sobre la historia clínica en todo el territorio del Estado español.

Debe señalarse también en esta materia que, a tenor de lo establecido en la Disposición Adicional Primera de la Ley, el Estado y las Comunidades Autónomas han de adoptar, en el ámbito de sus respectivas competencias, las medidas necesarias para la efectividad de la misma; ello implica, como señala De Lorenzo y Montero (2003) que, la regulación de la historia clínica gira en torno a tres instrumentos: la Ley de Derechos de los Pacientes, la de ejecución y desarrollo de dicha Ley por parte de las Comunidades Autónomas, y los protocolos pormenorizados en los centros sanitarios.

5.1.1 CONCEPTO DE HISTORIA CLÍNICA

La historia clínica es el relato patográfico o biografía patológica de la persona, esto es, la transcripción de la relación médico-paciente, por lo que ostenta un valor fundamental, no sólo desde el punto de vista clínico, sino también a la hora de juzgar la actuación del profesional sanitario. Lógicamente, la historia clínica es un documento en el que se expresa todo el proceso del enfermo, desde un punto de vista médico y en relación con la enfermedad que padece, desde que surge

la enfermedad hasta su alta médica; en ella se deben reflejar todos los datos médicos trascendentes para la curación del paciente.

Como señala Rodríguez López (2004), la historia clínica tiene como finalidad principal facilitar la atención o asistencia sanitaria del ciudadano, existen otras finalidades (gestión del sistema sanitario, supervisión e inspección del sistema sanitario, investigación clínica, investigación epidemiológica, judiciales, etc.), en principio subordinadas a la finalidad asistencial indicada. Desde esta perspectiva la historia clínica puede ser concebida como una suerte de biografía sanitaria de un usuario del sistema sanitario. Es el reflejo de la evolución sanitaria y vital del usuario, cuya identidad se plasma y puede ser extraída del conjunto de documentos que reproducen la historia clínica. Como todo relato vital, se trata de un relato pluridimensional y de un relato común.

Méjica García y Díez Rodríguez (2006:163) consideran a la historia clínica como: «el conjunto de información, único para cada paciente al menos en cada institución asistencial, que se redacta obligatoriamente por los médicos en beneficio del paciente, y que reúne la máxima integración de la información a él relativa, al que únicamente tienen acceso el paciente, los facultativos que intervengan en el tratamiento y las personas señaladas por la ley para fines de inspección sanitaria, científicos o docentes o a requerimiento de autoridad judicial, como expresión de los derechos a la intimidad personal y familiar y de las obligaciones de confidencialidad y secreto profesional por parte de todos los que tengan acceso al mismo, y en el que deben constar los datos fundamentales de la relación clínica, esto es, consentimiento y curso de la relación».

En consecuencia, no sirve únicamente para identificar al paciente, sino que incorpora los caracteres de otros sujetos que son relevantes en la configuración de la identidad clínica de aquel (profesionales sanitarios, familiares, etc.) Asimismo, no se limita a la exposición o descripción de hechos clínicos, y añade también valoraciones, decisiones, juicios clínicos, etc.

Pues bien, aunque la existencia de la historia clínica se remonta a lo largo de los tiempos, es solamente en época reciente –1947, en el Código de Nuremberg– cuando aparece el primer precedente de legislación de los derechos de los pacientes a la información. Tras estos primeros pasos surgieron informes de la *Joint Commission American*

(1970), posteriormente las Cartas de Derechos de los Pacientes de Francia, Consejo de Europa (1974) y la Declaración de Lisboa (1981) (Criado del Río, 1999).

En España se establecen normas concretas sobre la historia clínica y la regulación jurídica existente dimana de la Constitución Española (1978) y de la Ley General de Sanidad (1986) que, fundamentalmente en su artículo 10, en el que se recogen los derechos y obligaciones del paciente, regula el derecho a la información y a que quede constancia por escrito de su proceso asistencial. El artículo 61 de la misma Ley General establece la disponibilidad de la historia clínica por parte del paciente, de los médicos y de la Inspección Médica para fines científicos, y fija al mismo tiempo la obligatoriedad del secreto de aquellos que en función de sus competencias tienen acceso a la misma. En el Real Decreto 63/1995 de Ordenación de Prestaciones Sanitarias del Sistema Nacional de Salud de 10 de febrero establece como prestación la entrega de un ejemplar de la historia clínica, o bien determinados documentos, manteniendo la obligación de custodia de la misma por parte del centro sanitario (López González, 2000).

Según el artículo 14.1 de la Ley 41/2002 Básica de Autonomía de los Pacientes, «la historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos en el ámbito de cada centro».

Las notas que caracterizan a dicha definición son las siguientes: en primer lugar, la historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, ello significa que a diferencia de lo que sucedía con el artículo 61 de la Ley General de Sanidad[62] después de la promulgación de la Ley 41/2002 Básica de Autonomía de los Pacientes prevalece la información asistencial sobre cualquier información de otra índole. Llama la atención que el legislador, al definir la historia clínica, haya comprendido dentro de la definición el término «documentos», de lo que po-

---

[62] En el cual el conjunto de información relativa a cada paciente no solamente comprendía la información sanitaria sino también la información de carácter jurídico, económico, etc.

dría inferirse que la historia clínica solamente puede tener forma documental, olvidándose en la definición de la historia clínica informatizada[63], y de lo establecido en la Disposición Adicional Tercera[64].

En segundo término, es característico de la historia clínica la identificación en ella de los médicos y los demás profesionales que han intervenido, esta característica permite cumplir dos finalidades: da cumplimiento al derecho del paciente de que se le asigne un médico responsable de su caso y permite identificar, a efectos de responsabilidad patrimonial, al profesional sanitario que ha llevado a cabo su actuación de manera contraria a la *lex artis*. En tercer lugar, el objeto de la historia clínica es el de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos en el ámbito de cada centro (De Lorenzo y Montero, 2003).

Junto a la definición legal de la historia clínica se contienen disposiciones relativas al archivo de la misma, con la finalidad de garantizar la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura, adoptar medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental.

La historia clínica es uno de los documentos médicos más complejos que existen, debido a la multiplicidad de personas (médicos, diplomados en enfermería, personal sanitario, el propio paciente, sus familiares, etc.) y organismos (centros sanitarios públicos y privados,

---

63 Artículo 14.2 de la Ley 41/2002 establece que «Cada centro archivará las historias clínicas de sus pacientes, cualquiera sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información».

64 «El Ministerio de Sanidad y Consumo, en coordinación y con la colaboración con las Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición».

inspecciones de la Administración Sanitaria, Administración de Justicia, compañías de seguros, etc.) que en un determinado momento podrían estar interesados en tener acceso a los datos en ella contenidos, lo que comprometería la intimidad del paciente (Troncoso Reinaga, 2006).

Los distintos intereses con relación a la historia clínica pueden generar conflictos muy difíciles de resolver, tanto más cuanto que hasta ahora existía una gran dispersión de normas legales respecto a la misma, no se debe olvidar que los bienes y valores que se relacionan a la historia clínica son de una importancia extraordinaria ya que están directamente relacionados con derechos fundamentales de la persona como el derecho a la intimidad, a la salud, a la libertad y a la confidencialidad (León Sanz, 2004).

No obstante, ningún derecho es absoluto y, aunque el paciente tenga derecho a la intimidad y confidencialidad de los datos aportados en su relación médico-paciente, ante situaciones muy complejas, cuando el bien público o común prevalezca sobre el particular, el médico podrá, sin faltar al deber de secreto profesional, revelar los datos confidenciales del paciente; pero siempre lo hará de forma restringida, con discreción, revelando lo estrictamente justo y necesario, y haciéndolo exclusivamente ante quien proceda[65] (González Salinas *et al.*, 2004).

Bolivia aprueba la Norma Técnica para el manejo del Expediente Clínico mediante la Resolución Ministerial 0090 de fecha 26 de febrero de 2008 que define al Expediente Clínico como «el conjunto de documentos escritos e iconográficos evaluables que constituyen el historial clínico de una persona que ha recibido o recibe atención en un establecimiento de salud. Su manejo debe ser escrupuloso porque en él se encuentran todos los datos que nos permiten encarar de la mejor manera el estado de salud-enfermedad del paciente y su respectivo tratamiento» (artículo 5.1).

En relación a la definición de historia clínica el artículo 12.4 señala: «es el documento central del Expediente Clínico que a más de señalar los datos generales del paciente y sus antecedentes personales, familiares, no patológicos, patológicos y gineco-obstétricos en el caso de la mujer; describe las condiciones actuales de su estado de salud-

---

[65] Artículo 16.1 del Código de Ética y Deontología Médica (C.E.D.M.).

enfermedad, investigadas y recogidas a través de la anamnesis o interrogatorio y el examen físico general y especial. Concluye estableciendo el diagnostico presuntivo, diagnósticos diferenciales y una propuesta básica de conducta y tratamiento».

En Bolivia el término genérico que engloba una serie de documentos entre los cuales se encuentra la historia clínica es el «expediente clínico».

5.1.2 NATURALEZA JURÍDICA DE LA HISTORIA CLÍNICA

La naturaleza jurídica de la historia clínica ha sido, y seguirá siendo incluso después de la promulgación de la Ley Básica de Autonomía de los Pacientes cuestión debatida por la doctrina, pues de su determinación derivan aspectos tales como su eficacia probatoria, por ejemplo, el acceso a sus datos y el poder de disposición de éstos, las garantías de la intimidad y del secreto profesional y los límites que, por razones de interés público, pueden oponerse a su estricta observancia. Quiere decir con ello que en la historia clínica confluyen derechos e intereses jurídicamente protegidos, del médico, del paciente, de la institución sanitaria e incluso públicos que es preciso determinar y contrapesar para dar respuesta a los problemas planteados en la práctica (De Lorenzo y Montero, 2003).

La historia clínica es un documento, es decir, en los términos de la Ley 1/2000 de Enjuiciamiento Civil de 8 de enero, es un documento privado, pero un documento privado esencialmente médico-clínico, cuya finalidad principal, no única es la de facilitar asistencia sanitaria al paciente, recogiendo toda cuanta información clínica sea necesaria para asegurar, bajo un criterio médico, el conocimiento veraz, exacto y actualizado de su estado de salud, por el personal sanitario que lo atienda.

Pero también la historia clínica tiene en nuestros días un evidente valor probatorio en juicio, de tal suerte que puede ser un buen o mal reflejo del actuar del profesional, prueba de la existencia de un consentimiento informado debidamente prestado, o en definitiva, prueba de que el actuar profesional sanitario se ha conducido conforme a lo que demanda la *lex artis ad hoc*.

Partiendo de la doble consideración legal y ética de la historia clínica, uno de los aspectos más debatidos se centra en la cuestión de si la historia clínica constituye un documento público, polémica que viene referida a las historias clínicas elaboradas en el ámbito de las instituciones sanitarias públicas, ya que respecto de las producidas en consultas particulares no se plantea duda alguna en cuanto a su carácter privado. Lo discutible es si en función de la calidad o condición de facultativo autor de la misma se considera un documento público (expediente administrativo), o un documento privado (expediente particular). Resultando así que para un sector doctrinal no hay ninguna duda sobre la naturaleza de documento privado de la historia clínica, habida cuenta que en su redacción no se ejercen facultades de *imperium*. Pero para otra corriente, cuando la historia está elaborada en el ámbito de la decisión de la administración sanitaria goza por ello del carácter de documento público (Méjica García y Díez Rodríguez, 2006).

La valoración de los documentos que se lleva a cabo en un procedimiento judicial, según sean públicos, oficiales o privados, no es exactamente igual; sin embargo, cuando se procede a solicitar el envío de la historia o de copia de la misma (lo más habitual en la práctica diaria), sólo le interesa al funcionario que se ocupa de la redacción material del oficio consignar, con acierto el nombre de centro o dependencia a la que se ha de dirigir la solicitud para que llegue a su destino (Méjica García y Díez Rodríguez, 2006).

La Norma Técnica para el manejo del Expediente Clínico, aprobada por la Resolución Ministerial 0090 de fecha 26 de febrero de 2008, establece que el Expediente Clínico está integrado por dos partes una asistencial y otra administrativa.

El *contenido asistencial* incluye todos los documentos referidos al proceso salud enfermedad de la persona, durante la consulta, hospitalización y seguimiento ambulatorio, avalados por quienes participan en su atención. El *contenido administrativo* proporciona datos generales que permiten identificar en forma sencilla a cada paciente. Estos datos son: número del expediente clínico, fecha de ingreso, hora, nombre, ocupación, edad, fecha y lugar de nacimiento, sexo, raza, lugar de procedencia, domicilio, ocupación, teléfono (fijo o móvil), datos de los padres, familiar o persona responsable, seguro médico (si lo tuviese), servicio o unidad de hospitalización y n.° de cama ocupa-

da. Además, incorpora documentos (formularios) administrativos (artículo 11).

5.1.3 CONTENIDO DE LA HISTORIA CLÍNICA

El fin primordial de la historia clínica es facilitar la asistencia sanitaria al paciente recogiendo la información clínica necesaria para asegurar el conocimiento a los sanitarios que atienden al mismo, este objetivo es el único que puede justificar la creación y utilización de un soporte que trate datos como los utilizados en la misma.

Se busca que la historia clínica sea lo más completa posible, completa en cuanto a los contenidos de la historia debe referirse indistintamente a todas las fases de la atención sanitaria, incluyendo por lo tanto contenidos relativos al pronóstico, diagnóstico, tratamiento e incluyendo informaciones tan variadas como las ofrecidas verbalmente por el paciente, los resultantes de las pruebas diagnósticas o las apreciaciones del facultativo o facultativos intervinientes (Rodríguez López, 2004).

En términos genéricos, la estructura de la historia clínica viene determinada por:

1. Datos de carácter identificativo.
2. Datos clínicos.
3. Consentimiento del paciente o del representante legal, en su caso.

La Ley 41/2002, en su artículo 15.1 señala que: «la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente»; es decir, no se restringe la posibilidad de incorporar cualquier tipo de información siempre que sea veraz y necesaria. En el apartado 2 del mismo artículo dispone:

«La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud. El contenido mínimo de la historia clínica será el siguiente:

a) La documentación relativa a la hoja clínico estadística.

b) La autorización de ingreso.

c) El informe de urgencia.

d) La anamnesis y la exploración física[66].

e) La evolución[67].

f) Las órdenes médicas[68].

g) La hoja de interconsulta.

h) Los informes y exploraciones complementarias[69].

i) El consentimiento informado[70].

j) El informe de anestesia.

k) El informe de quirófano o de registro de parto.

l) El informe de anatomía patológica.

m) La evolución y planificación de cuidados de enfermería.

n) La aplicación terapéutica de enfermería[71].

---

66 Ordinariamente, la anamnesis se ordena en introducción, historial familiar, personal y social, historia de la enfermedad e historia sistemática, la exploración física o examen clínico, que abarca tanto la realizada por el profesional directamente como por los exámenes complementarios o auxiliares que el profesional prescriba o el paciente aporte debido a una exploración anterior.

67 Deben de recogerse las incidencias acaecidas durante el curso o evolución de la enfermedad: nuevos síntomas y signos, intensificación o remisión de los anteriores, complicaciones surgidas, respuesta al tratamiento, etc., es decir, configurar lo que puede denominarse como un auténtico diario clínico del estado de evolución del paciente.

68 Que comprenden el conjunto de instrucciones dadas por el facultativo durante el proceso asistencial.

69 Que deben comprender tanto los realizados con carácter complementario o coadyuvante de la exploración inicial en los procesos patológicos complicados, o cuando sean necesarios para la certeza y seguridad del diagnóstico, como los supuestos en los que el paciente en ejercicio del derecho que le otorga la Ley 16/2003 de Cohesión y calidad del Sistema Nacional de Salud de fecha 28 de mayo de 2003, haya ejercitado su derecho a una segunda opinión médica.

70 Como elemento esencial e integrante de la lex artis médica y presupuesto material de la actuación sanitaria, cuya omisión puede dar lugar a responsabilidad y obligación de indemnización por daños morales; en algunos casos, su ausencia incluso ha sido apreciada de oficio por los Juzgados y Tribunales.

71 Es el conjunto de cuidados y atenciones realizadas por el personal de enfermería bajo las indicaciones y órdenes dadas por los facultativos.

o) El gráfico de constantes.

p) El informe clínico de alta[72].

Los apartados b), c), i), j), k), l), ñ) y o) sólo serán exigibles en la cumplimentación de la historia clínica cuando se trate de procesos de hospitalización o así se disponga».

Como la información se transmite, como regla general, de forma verbal, hay que dejar constancia en la historia clínica, debiendo comprender como mínimo la finalidad y la naturaleza de cada intervención, sus riesgos y consecuencias. Asimismo, puede darse una situación en la que el daño que se prevé que cause la información a la persona sea de tal envergadura que claramente ello justifique la retención de la información; es el denominado *privilegio terapéutico* o *excepción terapéutica*, lo cual únicamente está justificado en circunstancias muy excepcionales; en el caso de que se tome esta decisión, el médico deberá dejar constancia razonada de las circunstancias en la historia clínica y comunicará su decisión a las personas vinculadas al paciente por razones familiares o de hecho, tal como venía sugiriendo la doctrina (León Sanz, 2004). Al tratarse de la historia clínica no sólo se enfrenta una obligación de los médicos y demás profesionales, sino se está ante un verdadero derecho que se atribuye a los pacientes.

La cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será responsabilidad de los profesionales que intervengan en ella (artículo 15.3 Ley 41/2002). Aunque la Ley 41/2002 no se refiere a la necesidad de que existan modelos normalizados de historia clínica, para cumplimentación de la misma se debe tender a la normalización en su estructura física y lógica.

La Disposición Adicional Tercera de la Ley 41/2002 establece que el Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de la Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y

---

[72] Refiere el informe emitido por el médico responsable en un centro sanitario al finalizar cada proceso asistencial de un paciente, debiendo especificar los datos de éste, un resumen de su historia clínica, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas.

tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, para evitar que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición.

Lo lógico sería que se establezca la obligatoriedad de una historia clínica única por paciente e institución que englobe de forma unitaria la documentación generada por la asistencia al enfermo tanto en el área de urgencias como en las áreas de consultas externas y de hospitalización.

El Reglamento de la Ley del Ejercicio Profesional Médico de Bolivia (Decreto Supremo 28562 de fecha 22 de diciembre de 2005) establece que para fines de atención, conciliación, arbitraje, proceso judicial u otros, el Expediente Clínico se organiza de la siguiente manera:

Durante la hospitalización:

— Gráficas de temperatura.

— Órdenes médicas.

— Evolución.

— Informes de laboratorio.

— Informe quirúrgico.

— Informe de anestesia.

— Informe de anatomía patológica.

— Notas de enfermería.

— Hoja de medicamentos.

— Historia y examen físico.

— Epicrisis.

— Informe de ingreso y egreso.

Secuencia de formularios de la historia clínica después del egreso:

— Informe de ingreso y egreso.

— Epicrisis.

— Historia y examen físico.

— Evolución.

— Órdenes médicas.

— Informes de laboratorio.

— Informe de anestesia.

— Informe quirúrgico.

— Informe de anatomía patológica.

— Gráficas de temperatura.

— Medicamentos.

— Notas de enfermería (artículo 12, D.S. N.º 28562).

La Norma Técnica para el Manejo del Expediente Clínico de Bolivia establece diferentes contenidos para el expediente clínico de hospitalización, de consulta externa y de emergencia (artículos 8, 9 y 10).

Tabla 6. Tipos de expediente clínico

Expediente clínico de hospitalización	Expediente clínico de consulta externa	Expediente clínico de emergencia
Es aquel que incluye todos los documentos relacionados con la enfermedad del paciente en el proceso de consulta externa y hospitalización, al cual se agregan los documentos de alta, una vez que se cumple la misma.	Es aquel que incluye los documentos relacionados con la enfermedad del paciente en el proceso de consulta externa realizado en el establecimiento, con o sin hospitalización. En el caso de derivación de otro establecimiento, para que se cumpla la consulta o consultas, contará con la respectiva documentación de referencia, y de darse el caso, copias de la documentación de resolución y contrarreferencia remitida al establecimiento de origen.	Es aquel que incluye todos los documentos relacionados con la atención y hospitalización del paciente, por el tiempo que permaneció internado en el Servicio o Unidad de Emergencias del establecimiento. Incorpora también la documentación referida al alta, referencia a otro servicio de internación (ya sea del propio establecimiento o de otro) y el certificado de defunción en caso de fallecimiento del paciente.
Lo conforman: a) Historia clínica propiamente dicha: datos generales y aspectos técnicos médicos b) Formulario de consentimiento informado. c) Órdenes médicas. d) Notas de evolución, interconsulta e informes de junta médica. e) Informes de exámenes de laboratorio, gabinete y anatomía patológica.	Lo conforman: a) Historia clínica propiamente dicha: datos generales y aspectos técnicos médicos b) Formulario de consentimiento informado. c) Órdenes médicas. d) Notas de evolución, interconsulta e informes de junta médica. e) Informes de exámenes de laboratorio, gabinete y anatomía patológica. f) Elementos de enfermería.	Lo conforman: a) Historia clínica propiamente dicha: datos generales y aspectos técnicos médicos b) Formulario de consentimiento informado. c) Órdenes médicas. d) Notas de evolución, interconsulta e informes de junta médica. e) Informes de exámenes de laboratorio, gabinete y anatomía patológica.

f) Elementos quirúrgicos: 1. Nota pre-quirúrgica (preoparatorio). 2. Protocolos quirúrgicos. 3. Nota pos-quirúrgica. g) Elementos de anestesia: 1. Nota pre-anestésica. 2. Protocolo de procedimiento anestésico (hoja de registro anestésico). 3. Nota posanestésica. 4. Nota de recuperación. h) Elementos de enfermería: 1. Notas de tratamiento y medicamentos administrados. 2. Hoja de evolución de enfermería. 3. Kardex de enfermería (en los expedientes clínicos de archivo). 4. Hoja de control de líquidos administrados y eliminados. i) Epicrisis. j) Documentos administrativos: 1. Nota de ingreso o admisión. 2. Nota de egreso o nota de alta (alta solicitada, transferencia). 3. Nota de referencia y contrarreferencia. 4. Informe de emergencias. k) Adicionales: 1. Protocolo de autopsia. 2. Certificado de defunción (copia). 3. Informes de auditoría médica especial o inducida. 4. Ficha social. 5. Autorización temporal. 6. Certificado médico (copia). 7. Recetas. 8. Formularios o fichas de programas específicos cuando corresponda (programa tuberculosis, enfermedades de transmisión sexual, quimioterapia, AIEPI, desnutrición, historia clínica perinatal, otros).	g) Notas de tratamiento y medicamentos administrados. h) Hoja de evolución de enfermería. i) Resumen de atención, orientación y prescripción del paciente. j) Documentos administrativos: 1. Nota de referencia y contrarreferencia. k) Adicionales. 1. Informe de auditoría médica interna especial o inducida. 2. Ficha social. 3. Certificado médico (copia). 4. Recetas. 5. Formularios o fichas de programas específicos cuando corresponda (programa tuberculosis, enfermedades de transmisión sexual, quimioterapia, AIEPI, desnutrición, historia clínica del CLAP y otros).	f) Elementos de enfermería: 1. Notas de tratamiento y medicamentos administrados. 2. Hoja de evolución de enfermería. 3. Kardex de enfermería (en los expedientes clínicos de archivo). 4. Hoja de control de líquidos administrados y eliminados. g) Resumen de atención, orientación y prescripción al paciente. h) Documentos administrativos: 1. Nota de ingreso o admisión. 2. Nota de egreso o nota de alta (alta solicitada, transferencia). 3. Nota de referencia y contrarreferencia. 4. Informe de emergencias. i) Adicionales: 1. Informes de auditoría médica interna especial o inducida. 2. Ficha social 3. Autorización

Fuente: Elaboración propia en base a la Norma Técnica para el Expediente Clínico

5.1.3.1 Condiciones básicas y características

En Bolivia el artículo 6 (Condiciones básicas del expediente clínico) de la Norma Técnica para el manejo del Expediente Clínico establece que el expediente clínico es un instrumento de interpretación y uso confiable, que debe cumplir las siguientes condiciones básicas:

a) *Veracidad:* Consiste en la descripción veraz de todo lo referente al estado de salud-enfermedad del paciente y los procedimientos realizados para su diagnóstico, tratamiento y rehabilitación.

b) *Carácter científico:* Consiste en el apego estricto a *la lex artis med*icae.

c) *Integridad:* Consiste en la presencia de datos clínicos suficientes sobre el estado de salud-enfermedad del paciente, complementados por métodos auxiliares de diagnóstico y tratamiento, junto a notas de evolución, tratamientos, consentimiento informado y documentos administrativos destacables de los procesos cumplidos durante la atención del paciente; refrendados todo con nombre, firma y sello o identificación escrita de las personas responsables.

d) *Sujeción a la norma:* Consiste en el estricto cumplimiento de la norma existente para la elaboración y manejo del Expediente Clínico, así como de la utilización de formularios u otros documentos expresamente diseñados para tales propósitos.

e) *Secuencialidad:* Esta referida a los registros de la atención, consignados en secuencia cronológica.

f) *Disponibilidad:* Es el acceso al Expediente Clínico en el momento en que se lo necesite, con las limitaciones que impone la norma.

g) *Exclusividad:* Se refiere a la existencia de un Expediente Clínico exclusivo y específico para cada paciente en el establecimiento donde es atendido. Puede tener carácter acumulativo, dependiendo de las veces que el paciente acuda a la consulta o sea internado, ya sea por causas de una misma enfermedad u otras.

h) *Unicidad:* Esta referida a la existencia de formatos únicos y generales de Expediente Clínico para todo el Sistema de salud, adecuados a los respectivos niveles de atención y las características propias de cada una de las especialidades existentes.

i) *Codificación:* Se refiere a la asignación de un nuevo número de identificación al Expediente Clínico que deberá ser único y el mismo para todos los documentos que lo constituyen y con el que figure en el archivo estadístico (artículo 6).

Méjica García y Díez Rodríguez (2006: 186-187) señalan que para que el expediente clínico pueda ser además un instrumento legalmente útil, que ratifique el testimonio de un profesional sobre su conducta clínica, facilite la valoración pericial y su defensa jurídica debe reunir los siguientes requisitos:

a) *Que resulten precisos:* El médico ha de ser específico y evitar términos vagos o poco concretos que puedan crear confusión tanto al «equipo médico» como el «equipo legal», ya que pueden significar cosas diferentes a personas distintas. Incluso lo que para el autor sea algo totalmente claro en el momento de escribirlo puede perder o cambiar el sentido de los que quiso expresar a la vuelta de unos años si se tiene que explicar ante un Juez.

b) *Que resulten legibles:* La historia clínica es un medio de comunicación, por lo que si no puede ser leída o es difícil de descifrar, la comunicación quedará dificultada y puede repercutir negativamente en la calidad de la asistencia prestada. De igual modo, si lo que se ha escrito es admitido como evidencia, puede ser leído por peritos, pero si éstos tienen dificultad en interpretarlo es posible que la versión sobre lo que se quiso decir sea diferente a la intención inicial del autor.

c) *Que resulten explicativos:* La historia clínica debe reflejar y reproducir la asistencia que se ha proporcionado al paciente y por qué se le ha dispensado; y debe ser capaz de explicar por qué se optó por una acción determinada (diagnóstico diferencial, pruebas diagnósticas, planes de tratamiento, etc.). Desde el punto de vista legal, el Juez buscará evidencias que apoyen lo que el médico está diciendo; por tanto, si la evidencia no está reflejada la historia clínica no le podrá ayudar. Por eso, el conocido formato S.O.A.P. (subjetivo, objetivo, análisis y plan) ha mostrado ser un buen método para justificar la asistencia proporcionada y crear un proceso lógico de actuación que se sostenga coherentemente ante un proceso judicial.

d) *Que resulten identificativos:* Es importante conocer la identidad de quién ha escrito la historia clínica, muchas de las historias no han podido utilizarse o no han tenido valor en la defensa de un caso por ser imposible descifrar quién las escribió, especialmente en aque-

llos hospitales donde un paciente suele ser visto por muchos médicos. Por lo que las anotaciones deben finalizar con la firma legible de quien atendió al paciente e incluso el cargo que tiene en ese momento y su número de colegiado. Y tan importante como la identificación del profesional es la identificación de paciente. Todas las hojas de la historia, resultados de pruebas complementarias, etc., deben identificar adecuadamente al paciente.

e) *Que resulten puntuales:* Conviene realizar las anotaciones con prontitud. Cuanto más se retrase en transcribir los comentarios, más información se olvidará. De igual modo, las percepciones cambian y se puede omitir información clave que debiera haberse incluido. Por eso se debe colocar fecha en cada anotación con el día, mes y año.

f) *Que resulten objetivos:* La historia clínica debe contener observaciones profesionales, objetivas, basadas en la anamnesis, exploración (inspección, palpación, percusión, auscultación) e información obtenida de las pruebas complementarias.

5.1.4 PROPIEDAD DE LA HISTORIA CLÍNICA

Más que debatir el problema de la historia clínica en sede del derecho de propiedad, parece más acertado hablar de distintos derechos concurrentes sobre la historia clínica, y de distintos titulares de esos derechos: de acceso, de disposición, utilización y de sus correlativas obligaciones: secreto y conservación. Y ésta ha sido también la posición del legislador al promulgar la Ley 41/2002 en la que no se pronuncia sobre la propiedad de la historia clínica y sí sobre el acceso a la misma (León Sanz, 2004).

Se han enunciado en la doctrina científica cuatro teorías sobre la propiedad de la historia clínica: teoría de la propiedad del paciente, teoría de propiedad del médico; teoría de la propiedad del centro sanitario y teoría integradora o ecléctica.

Como el paciente es la fuente de toda la información contenida en ella, pues aporta su propia información y su propia persona para su elaboración, él es el titular de la historia clínica. Los partidarios de la *teoría de la propiedad del paciente*, partiendo del dato básico de que la historia clínica se redacta en beneficio del paciente y del carácter fundamental y especialmente protegido de sus derechos en la relación

médico-paciente que se refieren a su intimidad, su identificación y su salud, sostienen que ésta es propiedad material del paciente, aunque no deje de reconocerse que este derecho puede no concebirse como un derecho de propiedad, sino de utilización de los datos contenidos en la historia clínica como si fuera suya (De Lorenzo y Montero, 2003).

García Hernández y Marzo Martínez (2000:1629 y ss.) defienden con una serie más acabada de argumentos que la historia clínica es de propiedad del paciente y no del médico:

1.º) Cuando el médico ejerce la profesión por cuenta propia en su consulta particular, el paciente arrienda sus servicios a cambio de un precio u honorarios. El servicio que adquiere es el acto médico, acto que comprende toda la actividad del médico, la cual debe sujetarse a la *lex artis*. Esta sujeción le obliga a redactar una historia clínica que recoge datos personales del paciente y que guardará hasta el término del contrato. Así, todos los actos que realiza el facultativo son remunerados por el paciente; es decir, el paciente compra la actividad del médico y parte de esa actividad es la historia clínica, que al término de la relación debe serle entregada. Esto es, el paciente adquiere la propiedad de todos los servicios arrendados, entre los que se incluye la historia clínica, historia que se incorpora a su patrimonio con todas las facultades características de la propiedad (de uso, disfrute y disposición), facultades de las que no dispone el médico; del médico serán los estudios, dictámenes, publicaciones, etc., que elabore fuera de esa relación de servicios. Otra cosa es que el médico no entregue la historia clínica al paciente; en tal caso tendrá la posesión pero nunca la propiedad, ni tampoco la custodia en términos contractuales.

2.º) Si el facultativo realiza su actividad por cuenta ajena mantendrá una relación contractual en la que una parte se obliga a realizar determinados servicios para otra, bajo el ámbito de su poder de organización y dirección a cambio de un salario como contraprestación de ese trabajo. El contrato de trabajo tiene como elementos característicos el de ser oneroso, conmutativo y sinalagmático. Ser conmutativo implica que la actividad del médico pertenece al empleador, el cual, a cambio de ese hacer y su obra, entrega al médico una retribución (carácter oneroso), estableciéndose así entre ambos una relación bilateral o sinalagmática. El médico en ese hacer efectúa actos médicos, entre ellos la historia clínica, que debe entregar al emplea-

dor en tanto titular del centro médico u hospital, sea público o privado. De este modo, la historia clínica no sería nunca del médico, sino en su caso del centro sanitario, pero como quiera que al centro sanitario le paga el paciente de forma directa (centros privados) o indirecta (centros públicos) por recibir una actividad médica en la que se incluye la historia clínica, ésta será de propiedad exclusiva del paciente y no del médico ni del hospital.

Los partidarios de la *teoría de la propiedad del médico* destacan su carácter de propiedad intelectual y científica que aporta el facultativo en el proceso de diagnóstico y tratamiento del paciente, de manera que toda la historia se encontraría tejida de juicios personales y que, como conjunto, es objeto de tutela por la Ley de Propiedad Intelectual y disposiciones que desarrollan ésta. Pero, sin embargo, el principal inconveniente de esta teoría radica en que la Ley de Propiedad Intelectual establece que en el caso de facultativos que prestan sus servicios por cuenta ajena, se transmiten al empresario los frutos e invenciones del trabajador, aparte de que la historia clínica no encaja en el objeto de tal propiedad intelectual (De Lorenzo y Montero, 2003 y León Sanz, 2004).

Es importante tener presente que el médico que asiste al paciente es el que genera y crea la historia clínica y, en consecuencia, dentro de cada proceso asistencial, el médico correspondiente tiene acceso a dicha historia, y dentro de dicha historia clínica, a la totalidad de los documentos que la integran y que le servirán de antecedentes a la hora de diagnosticar y tratar al paciente (Moreno Vernis, 2002).

León Sanz (2004) señala que solamente existe una excepción que justificaría la propiedad de la historia clínica a favor del médico que la realiza, y sería en supuestos de asistencia psiquiátrica con complejas elaboraciones psicodinámicas, en cuyo caso el autor debería hacer una reserva expresa de su obra en documento aceptado por ambas partes (médico y centro).

Así, Criado del Río (1999) defiende la idea de que el ejercicio privado de la medicina hace al médico propietario de la historia clínica, y que en casos de médicos empleados en centros públicos o privados, el propietario de la historia clínica pasa a ser el centro sanitario, señalando además que la tesis de que el paciente no es el propietario de la historia clínica no es incompatible con su derecho de acceso, aunque con ciertas limitaciones.

Méjica García y Díez Rodríguez (2006:175) coinciden con Romeo Casabona y Castellano Arroyo en las dudas acerca de que la historia clínica pudiera considerarse como «creación literaria, artística o científica» y por ende tributaria de protección por la Ley de Propiedad Intelectual de España[73] (en la actualidad, el texto refundido aprobado por el Real Decreto Legislativo 1/1996 de 12 de abril). Todo ello resulta incuestionable para la sentencia de la Audiencia Provincial de Valencia de junio de 1995, que declaró que la historia clínica no puede ser calificada como propiedad del facultativo al no resultar encajable en la enumeración que se contiene en los artículos 10 a 12 de la Ley de Propiedad Intelectual ni permitir su objeto la catalogación como creación original.

Los defensores de la *teoría de la propiedad del centro sanitario* arguyen que la historia clínica debe de obtener la máxima integración posible, al menos en el ámbito de cada centro; habida cuenta que es también el centro sanitario el que proporciona el soporte de la historia clínica y el que está obligado a conservarla, se utilizan todas estas características para demostrar dicha propiedad.

Con carácter general, se fundamenta esta teoría en tres presupuestos:

a) Que el derogado artículo 61[74] de la Ley General de Sanidad (LGS) de España establecía que la historia clínica debe ubicarse en el

---

73 La reforma de la Ley de Propiedad Intelectual (LPI) ya es realidad. Han sido años de debates y críticas tras los que el Partido Popular ha aprovechado su mayoría absoluta en el Parlamento para sacar adelante en solitario la normativa, el texto entra ahora en vigor. La reforma, eso sí, es parcial, hasta el punto de que establece un plazo de un año para que el Ejecutivo apruebe otra modificación, más profunda y completa, de la ley. Aun así, y pese a que algunas de las novedades entrarán en vigor paulatinamente a lo largo del año, la nueva LPI contiene cambios de cierto calado que han provocado consecuencias incluso antes de ser aplicables. El País (2015): «*Claves de la nueva Ley de Propiedad intelectual*» [en línea]: http://cultura.elpais.com/cultura/2015/01/05/actualidad/1420459097_337231.html [Consulta: 15/09/2015]

74 Artículo 61: «En cada Área de Salud debe procurarse la máxima integración de la información relativa a cada paciente, por lo que el principio de historia clínico-sanitaria única por cada uno deberá mantenerse, al menos, dentro de los límites de cada institución asistencial. Estará a disposición de los enfermos y de los facultativos que directamente estén implicados en el diagnósti-

marco del Área de Salud, que son demarcaciones estrictamente administrativas, según el artículo 56.2 de la LGS.

b) Que es el centro sanitario el que proporciona el soporte de las historias (papel, software, etc.) y el que está obligado a su custodia y conservación, por lo que puede decirse que son del hospital.

c) Que cuando la actividad del médico se realiza por cuenta ajena, bien sea en un centro sanitario de titularidad pública o en un centro privado, el ordenamiento jurídico atribuye al empresario la titularidad sobre las denominadas invenciones del trabajador. Consecuentemente, se produce la cesión de los frutos de la actividad productiva al empleador y por tanto, la titularidad de la historia clínica corresponde a la institución pública o privada en el que se realiza (Méjica García y Díez Rodríguez, 2006).

Por último, señala De Lorenzo y Montero (2003), a las *teorías integradoras o eclécticas de la propiedad* de la historia clínica, a la vista de los insatisfactorios resultados a los que se llega con las anteriores posiciones, recogen los puntos de vista derivados de dos o más de ellas para tratar de armonizarlos, de tal modo que podría hablarse de una propiedad compartida de la historia clínica: del médico, del paciente y de la institución. Es la postura que parece que alcanza mayor predicamento, trata de recoger parcialmente las teorías antes citadas armonizándolas. Los partidarios de esta tesis señalan gráficamente que el propietario de la historia clínica es el centro sanitario; el paciente es el titular de la intimidad en ella reflejada, y el médico, dueño de su aportación intelectual y administrador del interés de terceros allí registrados.

Subyacente a esta corriente conciliadora está la constatación de que la historia contiene componentes heterogéneos desde el punto de vista jurídico. Así, Romeo Casabona y Castellano Arroyo (1993) citados por Méjica García y Díez Rodríguez, (2006:179) han distinguido, en primer lugar, los relativos a la organización y gestión administrati-

---

co y tratamiento del enfermo, así como a efectos de inspección médica o para fines científicos, debiendo quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica. Los poderes públicos adoptarán las medidas para garantizar dichos derechos y deberes».

va y económica del centro sanitario; en segundo lugar, los que se refieren a los datos identificadores del paciente y otros directa o indirectamente relacionados con su enfermedad aportados por el paciente, y por último los resultados de las exploraciones realizadas por el médico, en la medida que comporten un juicio deductivo derivado de los conocimientos profesionales del facultativo, así como la emisión del juicio diagnóstico y pronóstico, la prescripción del tratamiento y su evolución; también habría que añadir las anotaciones subjetivas del médico en relación con las reacciones y actitudes del paciente, que son de especial importancia por ejemplo en el ámbito psiquiátrico.

En todo caso, hacer depender de la propiedad de la historia clínica la totalidad de su problemática actual puede conducir a resultados desproporcionados, por lo que resulta mucho más realista destacar su carácter instrumental y su finalidad primordial: la constancia de la información clínica y terapéutica así como la puesta a disposición de la misma en beneficio de la salud del paciente (Rodríguez López, 2004).

Se debe tener presente que el paciente es un eje fundamental de la historia clínica, y no puede negarse la incidencia que tiene sobre su persona, esto obligaría a contemplar la historia clínica desde una perspectiva diferente. Se estaría ante un soporte de la historia vital de una persona, la cual, como centro de la historia clínica, también debería tener derecho a determinar para qué y cómo debe ser utilizada la citada historia.

En definitiva, lo que postulan estos autores es que se está ante una propiedad compartida, o, más precisamente, ante una cotitularidad de derechos sobre un único objeto, la historia clínica.

En Bolivia el Reglamento para la elaboración, manejo y archivo del expediente médico o clínico en las entidades de la Seguridad Social a Corto Plazo aprobado mediante Resolución Administrativa 158 – 2005 de fecha 28 de diciembre de 2005 del Instituto Nacional de Seguros de Salud (INASES) establece que el expediente clínico es un documento médico legal de propiedad del establecimiento de salud (hospital, policlínico, clínica o centro de salud) y por consiguiente ningún funcionario puede retirarlo fuera de la institución o utilizarlo sin la autorización por autoridad respectiva. Solo en caso de requerimiento por autoridad competente pueden emitirse fotocopias autentificadas por la Unidad Jurídica de la entidad y avaladas por el Direc-

tor del establecimiento de salud según Resolución Ministerial 028/97 (artículo 12).

5.1.5 ARCHIVO DE LA HISTORIA CLÍNICA

Las historias clínicas se archivan y se conservan fundamentalmente para garantizar una asistencia adecuada al paciente, pero también con fines docentes, de planificación, organización, gestión y evaluación de la actividad asistencial, por aspectos jurídico-legales y como fondo histórico documental. Cada centro sanitario será, por ley, el responsable del adecuado archivo, conservación y disponibilidad de la historia clínica debiendo garantizar su seguridad y protección, estableciendo las normas concretas que lo hagan posible.

Como en la historia clínica pueden ser usados cualquiera de los soportes documentales adecuados para su utilización, siempre y cuando garanticen la autenticidad, integridad, seguridad y conservación; cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información (artículo 14.2 Ley 41/2002). Es lógico esperar que en esta sede se intente que la historia clínica sea completa y se encuentre ordenada (Rodríguez López, 2004).

Las Administraciones sanitarias establecerán los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura (artículo 14.3 ley 41/2002). No obstante, no se dispone nada sobre el tipo de mecanismo a utilizar. El desarrollo de esta norma deberá tener en cuenta el contenido de la Ley 41/2002, y deberá tender a facilitar el acceso del paciente a dicha historia (Moreno Vernis, 2002).

Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental (artículo 14.4 Ley 41/2002). La mayor parte de las normas autonómicas ya contenían reglas similares.

Posterior a la Ley 41/2002, el artículo 56 de la Ley 16/2003, de cohesión y calidad del Sistema Nacional de Salud establece:

«Con el fin de que los ciudadanos reciban la mejor atención sanitaria posible en cualquier centro o servicio del Sistema Nacional de Salud, el Ministerio de Sanidad y Consumo coordinará los mecanismos de intercambio electrónico de información clínica y de salud individual, previamente acordados con las Comunidades Autónomas, para permitir tanto al interesado como a los profesionales que participan en la asistencia sanitaria el acceso a la historia clínica en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información, cualquiera que fuese la Administración que la proporcione.

El Ministerio de Sanidad, Servicios Sociales e Igualdad establecerá un procedimiento que permita el intercambio telemático de la información que legalmente resulte exigible para el ejercicio de sus competencias por parte de las Administraciones públicas.

El intercambio de información al que se refieren los párrafos anteriores se realizará de acuerdo con lo dispuesto en la Ley Orgánica 15/1999 de 13 de diciembre y en la Ley 41/2002, de 14 de noviembre».

La disponibilidad de la historia clínica obliga a los responsables del centro sanitario, y de manera especial a los del archivo, a adoptar procedimientos de utilización en función de los motivos que justifiquen el uso de la misma. Para favorecer el procedimiento de archivo y almacenamiento de historias, se puede crear un archivo pasivo de historias donde estarían archivadas o almacenadas todas aquellas historias correspondientes a pacientes fallecidos, pacientes cuyas historias no hubieran sido movilizadas o utilizadas en el número de años que se determine desde el último episodio asistencial, o las de pacientes que fueron asistidos puntualmente en un hospital, pero que pertenecen a áreas sanitarias distintas y distantes a la que prestó la asistencia. Este archivo pasivo estaría físicamente lo más próximo posible al archivo activo en el que se almacenarían las historias clínicas de los pacientes hospitalizados, las de las consultas externas y aquellas con un movimiento inferior al número de años determinado desde el último episodio asistencial (León Sanz, 2004).

La historia clínica deberá ser archivada íntegramente. Cuando los motivos asistenciales o de otra naturaleza, debidamente fundamenta-

dos, se precisen duplicar el contenido total o parcial de la misma, se procederá a la reproducción del material estrictamente necesario, quedando los originales en el archivo de historias clínicas. Si además, se precisara de una custodia especial, la historia clínica original se archivará bajo llave, y la copia obtenida reemplazará al original en el archivo normalizado. Para asegurar el cumplimiento de las normas deontológicas respecto al secreto médico, acceso y manejo de la historia clínica, el Código de Ética y Deontología Médica estima que el responsable del archivo de historias clínicas y de los bancos de datos ha de ser un médico.

En Bolivia el Reglamento para la elaboración, manejo y archivo del expediente médico o clínico en las entidades de la Seguridad Social a Corto Plazo aprobado mediante Resolución Administrativa 158 – 2005 de fecha 28 de diciembre de 2005 del Instituto Nacional de Seguros de Salud (INASES) establece sobre el archivo del expediente clínico que:

a) Los expedientes clínicos deben ser conservados por un periodo de cinco años en archivo a partir del último acto médico.

b) A partir del sexto año, la institución puede organizar sus archivos en depósitos, medios magnéticos u otros que la tecnología pueda proporcionar teniendo en cuenta que se debe contar con un resumen de todos sus expedientes clínicos.

c) El área de archivo debe ser un espacio que brinde seguridad a los expedientes con el equipo, mobiliario suficiente y tener la señalización correcta para el manejo por índice alfabético o código de acuerdo al procedimiento que se decida emplear.

d) Debe contar con un registro único y confiable (listado de expedientes) o con una metodología de archivo de acuerdo a las características de cada entidad gestora, que permita identificar con facilidad la ubicación de los expedientes requeridos al momento necesario.

e) Debe designarse un responsable de archivo con formación en el tema y cuyas funciones están establecidas en el manual de funciones y reglamento interno de la entidad (artículo 14).

La Norma Técnica para el manejo del Expediente Clínico de Bolivia establece que, respetando las particularidades técnicas de archivo de cada establecimiento, los Expedientes Clínicos los custodia la *Unidad de Archivo y Estadísticas*, en un único archivo central con dos

grandes divisiones: activo y pasivo. Se define *archivo pasivo* al que contiene los expedientes clínicos de las defunciones, y *archivo activo* el que contiene los expedientes clínicos en secciones que corresponden a los servicios de hospitalización, colocados en orden alfabético según el primer apellido del paciente y manteniendo el mismo código o número que se asignó al Expediente Clínico del paciente en la primera consulta o internación realizada en el establecimiento (artículo 30).

Algunos expedientes clínicos que requieren mayor custodia se archivan en sección especial en los siguientes casos:

a) Expedientes clínicos solicitados por tribunales de justicia.

b) Expediente clínico sujeto a auditoría externa.

c) Expediente clínico sujeto a peritaje.

d) Expediente clínico sujetos a procesos administrativos.

e) Expediente clínico que a juicio del médico tratante y con autorización del Director del establecimiento requieran de esa medida (artículo 32).

5.1.6 CONSERVACIÓN Y CUSTODIA DE LA HISTORIA CLÍNICA

Se debe partir de una base imprescindible: la obligación de conservar y custodiar la historia clínica es un deber consustancial a la praxis médica. Lógicamente, la conservación de la historia clínica debe orientarse a preservar la información clínica que contiene y no, necesariamente, el documento original.

El Grupo de Expertos en Información y Documentación Clínica[75] ha llegado al consenso de que la custodia de la historia clínica, y por tanto de la información en ella contenida cuando la asistencia se realiza por médicos adscritos laboralmente a un centro sanitario, es responsabilidad de la dirección del centro. En caso contrario, esta responsabilidad recae directamente sobre el médico que realiza dicha asistencia. La conservación debe orientarse a preservar la informa-

---

[75] Grupo de Expertos en Información y Documentación Clínica (1997). «*Documento final del Grupo de Expertos*», noviembre de 1997. Ministerio de Sanidad y Consumo. Madrid.

ción clínica y no necesariamente el documento (soporte) original en que se generó. Este Grupo defiende que la finalidad principal de la conservación de la información clínica es facilitar la asistencia sanitaria de la persona titular de los datos (Sánchez Carazo, 2000).

De lo anterior, se concluye que la responsabilidad sobre la historia clínica corresponde a la dirección del centro cuando la asistencia se realiza por médicos y otros profesionales sanitarios que trabajen en el sistema público o contratados en centros, así en el caso de que a un médico se le suspenda un contrato, las historias de sus pacientes permanecerán en el centro. El médico que deja de prestar servicios en una institución sanitaria privada no tiene potestad para llevarse las historias clínicas de sus pacientes porque esos datos pertenecen al propio centro. Sin embargo, cuando no se trata de un centro sanitario sino de un conjunto de consultas, el médico, si se traslada, puede llevar consigo las historias clínicas. Es decir, que propiedad y custodia de la historia clínica van de la mano (Méjica y Díez, 2006).

La seguridad de la historia clínica manual es muy importante, no sólo por lo que supone vulneración de la intimidad, sino también porque la pérdida de datos sanitarios puede incidir en la futura salud del paciente y, tanto en centros públicos como privados las historias clínicas necesitan protección.

La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud, su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas (artículo 17.2 Ley 41/2002). Hay que tener presente que son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (artículo 17.6 Ley 41/2002).

Los profesionales sanitarios tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes (artículo 17.3 Ley 41/2002).

La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la Unidad de Admisión y Documentación Clínica, encargada de integrar en un sólo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario (artículo 17.4 Ley 41/2002).

Respecto a la custodia de la historia clínica, el paciente tiene derecho a que los centros sanitarios establezcan mecanismos de custodia activa y diligente de las historias clínicas. A través de dicha custodia se permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad (artículo 19 Ley 41/2002).

Un aspecto de la Ley 21/2002 que resulta problemático es el de la conservación de la documentación clínica. Como consecuencia de la aplicación de la LOPD a los datos informatizados, y también a los datos susceptibles de informatización, se prevé en la nueva ley que los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado en cada caso y, como mínimo, de cinco (5) años contados desde la fecha del alta de cada proceso asistencial (De Lorenzo y Montero, 2003).

Este plazo mínimo de conservación de la historia clínica de cinco (5) años presenta el problema de que, si se tiene en cuenta que la historia clínica también sirve como medio de prueba en los procesos judiciales sobre responsabilidad profesional, y asimismo, que la Ley 41/2002 resulta de aplicación a los centros sanitarios públicos y privados, en el caso de que se accione contra un profesional sanitario, por presunta responsabilidad contractual, el plazo de prescripción de la acción de responsabilidad contractual es de quince (15) años, y en el caso de que la historia clínica hubiera sido destruida transcurridos cinco (5) años desde el último proceso asistencial, el profesional sanitario no tendría forma de probar que su actuación no fue contraria a Derecho (Troncoso Reinaga, 2006).

Hoy en día se están realizando conciertos y contratos para la custodia y depósito extrahospitalario de la documentación clínica, incluso existen empresas especializadas en esta materia (Sánchez Carazo, 2000). Los centros asistenciales que, por lo general, se mueven con limitaciones de espacio y recursos, no pueden, en una gran parte de los casos, asumir la conservación indefinida del archivo; por ello, para lograr el objetivo de mantener los expedientes clínicos una vez que han dejado de tener interés para una posible continuación asistencial, están obligados a orientar esfuerzos de todos hacia la adopción de fórmulas que pueden facilitar la transferencia de esta documentación a determinadas instituciones, distintas a las sanitarias, que puedan, de alguna manera, dedicarse al cuidado y conservación de las historias clínicas (Rodríguez López, 2004).

La delegación de la custodia solamente se debería realizar cuando el centro no disponga de espacio físico suficiente ni de personal adecuado, por lo que este mecanismo nunca debería utilizarse para almacenar los datos informatizados. Con independencia del derecho de acceso a los episodios asistenciales que se reflejan en la historia clínica, así como el acceso motivado de terceros cuando invoquen derechos o intereses legítimos, es el centro sanitario el titular de la historia clínica y, en consecuencia, el obligado a su conservación y custodia, así como a la administración y gestión de la información incorporada a la historia clínica, de tal manera que una conducta negligente en cualquiera de estas obligaciones puede generar la responsabilidad patrimonial del centro (Álvarez-Cienfuegos, 2000). Estas competencias no son delegables ni renunciables, pues constituyen parte de las obligaciones que el sistema de salud asume con los ciudadanos al garantizar la asistencia sanitaria.

La Norma Técnica para el manejo del Expediente Clínico de Bolivia (Resolución Ministerial 0090 de fecha 26 de febrero de 2008) establece que mientras dure el episodio de asistencia en consulta u hospitalización, el Expediente Clínico permanecerá en los distintos servicios y será responsabilidad de los mismos su custodia: a) Expedientes clínicos procedentes de urgencias en 24 horas; b) Expedientes clínicos procedentes de altas de hospitalización en 48 horas y; c) Expedientes clínicos procedentes de consultorio externo en 24 horas. Para cualquier otra eventualidad que pudiese presentarse, el plazo de devolución nunca superará las 72 horas (artículo 29).

Para la conservación del Expediente Clínico el artículo 31 establece: «el contenedor para la conservación y archivo del Expediente Clínico, ya sea durante la internación del paciente o para su mantenimiento indefinido en la Unidad de Archivo y Estadísticas, debe ser de material impermeable, opaco, impenetrable a rayos solares, con cierre hermético que evite la caída o pérdida de documentos, con un recuadro exterior que permita consignar los datos más importantes para fines de ordenamiento y clasificación, y de un tamaño lo suficientemente grande como para contener toda la documentación, incluidas placas radiográficas o tomográficas de formato mayor».

Algunos Expedientes Clínicos que requieren mayor custodia, se archivarán en sección especial, en los siguientes casos: a) solicitados por tribunales de justicia; b) sujetos a Auditoría Médica Externa; c) sujetos a Peritaje; d) sujetos a procesos administrativos y; e) que a juicio del médico tratante, y que con autorización del director del establecimiento, requieran de esta medida (artículo 32).

El Expediente Clínico extraviado es aquel que no aparece en el Archivo Central, pese a la constancia de su entrada y colocación en la división y sección correspondiente, según los propios registros del Archivo. Pasado un mes, si el Expediente Clínico no apareciera pese a las investigaciones que fuesen realizadas, se notificará el extravío a la dirección del establecimiento, con una copia que quedará como constancia en una carpeta específica de la documentación administrativa del Archivo (artículo 34).

Finalmente, la Unidad de Archivo y Estadística del establecimiento debe cotejar diariamente el listado de los pacientes egresados con los expedientes clínicos recibidos para su correspondiente archivo, lo cual le permitirá identificar aquellos expedientes clínicos que estuvieren retenidos en los servicios de consulta externa y hospitalización donde se esté dando la retención, quién en un plazo máximo de 24 horas hábiles hará efectivo el envío del Expediente Clínico retenido (artículo 35).

5.1.7 ACCESO A LA HISTORIA CLÍNICA

Algunas de las principales dudas que surgen en torno a la regulación de la historia clínica giran en torno al acceso a la misma, la his-

toria clínica es el documento sanitario que contiene más información íntima de un paciente y su uso constituye un bien irrenunciable de cada persona en su atención como enfermo y también para el desarrollo de la lucha contra la enfermedad y en la promoción de la salud. Concurre en la ordenación de la historia clínica tanto el interés individual de cada paciente respecto de su salud como el interés general de la sociedad en la lucha contra la enfermedad, pudiéndose vincular este último, además, a los usos extra sanitarios de la historia clínica (Martí y Pidevall, 2004).

Respecto al alcance del derecho al acceso a la historia clínica es necesario conectar la atribución de este derecho a la finalidad que lo justifica, siendo ésta la adecuada asistencia al paciente, por lo que cualquier acceso cuya finalidad sea distinta de la indicada no debería producirse, y en su caso no estará amparado por el ordenamiento jurídico vigente dando lugar a vulneración de la intimidad del paciente.

Se puede distinguir entre los siguientes sujetos legitimados para el uso de la historia clínica, y por consiguiente entre los siguientes grupos de personas legitimadas que en distinto grado pueden acceder a la misma: paciente; médicos y otros profesionales sanitarios; personal de la administración; otras personas vinculadas al paciente en caso de fallecimiento; inspectores sanitarios; terceras personas con finalidades judiciales, epidemiológicas y de investigación o docencia (De Lorenzo y Montero, 2003; Jañez Ramos *et al.*, 2002; y Martí y Pidevall, 2004).

El paciente amparado por el derecho de información que la Ley General de Sanidad de España le reconoce, tiene derecho a acceder al contenido de la historia clínica, cuando así lo estime oportuno y solicite. El artículo 10.5 de la Ley General de Sanidad establece que todo ciudadano tiene derecho con respecto a las distintas Administraciones públicas sanitarias a que se le dé información completa y continuada verbal y escrita sobre su situación médica, incluyendo diagnóstico, pronóstico y alternativas de tratamiento. Por lo tanto, se entiende que todo paciente tiene derecho a acceder a su historia clínica cuando así lo estime necesario (Jañez Ramos *et al.*, 2002).

En efecto, tras la promulgación de la Ley 41/2002 Básica de Autonomía de los Pacientes, sigue sin quedar claro hasta dónde puede acceder el paciente a la misma. Como principio general, el paciente tiene derecho al acceso a la historia clínica y a obtener copia de los

datos que figuran en ella con los siguientes límites: a) Datos de terceros cuyo derecho a la confidencialidad pueda verse afectado de darse el acceso al paciente a la historia clínica que los contiene y b) Anotaciones subjetivas de los profesionales que han intervenido en la historia clínica, cuando así lo disponga el propio profesional (Martí y Pidevall, 2004).

Sin embargo, este acceso de los profesionales a la historia clínica no es uniforme puesto que la Ley 41/2002 prevé que cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten, pudiendo ser, obviamente, distintos métodos de acceso entre los diferentes centros sanitarios.

En el caso de que el paciente sea capaz y está vivo solamente podrá entregarse los datos sanitarios a personas que se encuentren expresamente autorizadas por el propio paciente. En este sentido hay que recordar que, pese a que el derecho a la intimidad es irrenunciable, si cabe que su titular consienta que terceras personas accedan a su ámbito de privacidad. Así, las personas autorizadas explícitamente por el paciente pueden acceder a sus datos sanitarios (Méjica y Díez, 2006).

Si el paciente solicita el original de las pruebas diagnósticas practicadas integrantes de la documentación clínica se recomienda conservar copia de la misma y hacer constar en la historia clínica que el original ha sido entregado al paciente. En cuanto al acceso a la historia clínica mediante representante previsto en la Ley 41/2002 son de aplicación las reglas generales sobre atribución y prueba de la representación, admitiéndose, en principio, tanto los poderes de representación verbales como escritos (Martí y Pidevall, 2004).

Por otro lado, no cabe duda alguna de que, al tratarse la historia clínica de un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente, los profesionales asistenciales del centro sanitario, que tienen como función diagnosticar y tratar al paciente, tienen acceso pleno a la misma como instrumento fundamental para su adecuada asistencia, hallándose además obligados por el secreto profesional. El acceso a la misma llega a constituirse para el profesional en un derecho y a la vez que en una obligación, en cuanto se le impone el deber de conocer toda la información relativa a su

paciente para el mejor desarrollo de la actividad asistencial (De Lorenzo y Montero, 2003).

Las limitaciones de acceso a la historia clínica se fundamentan en el carácter confidencial que tiene la historia clínica, con todos sus componentes (anamnesis, exploración física, curso clínico, gráficas, dictámenes de exploraciones radiológicas, analíticas, etc.). Así todos los profesionales sanitarios que acceden a la historia clínica en el ejercicio de su actividad están obligados a mantener la confidencialidad. El enfermo que proporciona la información sobre su vida y salud lo hace solamente para obtener un diagnóstico y fijar un tratamiento por lo que cualquier uso distinto del anterior exigirá su consentimiento (Calvo Sánchez, 2006).

Es destacable que la autorización recae exclusivamente en personal sanitario, el que a su vez tiene un específico deber de secreto, con la finalidad de reforzar las garantías de confidencialidad y buen tratamiento de la información que deben presumirse de cualquier profesional sanitario (Martí y Pidevall, 2004).

La Resolución Ministerial 0090 que aprueba la Norma Técnica para el manejo del Expediente Clínico de Bolivia señala que ni ética ni jurídicamente es admisible impedir que el paciente tenga acceso a su Expediente Clínico las veces que lo requiera, ya sea por solicitud directa o por intermedio de su tutor jurídicamente responsable si se encuentra internado, o a través de solicitud notariada dirigida al Director del establecimiento si no está internado. En tales casos, el Director accederá a la solicitud, disponiendo la entrega –según posibilidades de la institución– ya sea de una copia magnética o de una copia fotostática del Expediente Clínico del paciente, debidamente firmada y sellada en cada uno de sus folios, cotejados con los originales en presencia del paciente o su representante legal. Todo este procedimiento constará en el levantamiento de un acta de entrega, que será firmada por el paciente o su representante legal y por el Director del establecimiento, en copias para ambas partes (artículo 23).

El requerimiento del Expediente Clínico puede tener causas legales, auditoria médica externa o peritaje:

— *Requerimiento por causa legal:* El Director del establecimiento dará curso al requerimiento, siempre y cuando provenga de autoridad Judicial o Fiscal competente, con levantamiento de un Acta de Entrega-Recepción, que será firmada tanto por la parte

solicitante como por el Director, y con el único recaudo de sacar una copia magnética o fotostática del Expediente Clínico para el establecimiento, hasta que el original sea devuelto mediante llenado de un Acta de Devolución (artículo 24.1).

— *Requerimiento por Auditoría Médica Externa:* El Director del establecimiento dará curso al requerimiento de acuerdo a los recaudos contemplados en los artículos 54[76] y 55[77] del Manual de Auditoria en Salud y Norma Técnica para su realización (artículo 24.2).

— *Requerimiento por peritaje:* Se cumple con el mismo procedimiento establecido para requerimientos por causa legal (artículo 24.3).

Los responsables de docencia deben elaborar modelos o prototipos especiales de Expediente Clínico por patologías, habituando al estudiante a su correcto manejo, sin afectación o perjuicio de las labores asistenciales del establecimiento, de la presente norma, ni el derecho a la privacidad, reposo y confidencialidad que tienen los pacientes (artículo 22).

A la significación documental médico-legal que tiene el Expediente Clínico en Bolivia, se agrega su carácter confidencial dentro de los alcances éticos y de respeto a los derechos de los pacientes. Por tal razón, su manejo es restringido al grupo de personas que tienen la responsabilidad directa del paciente y que deben estar claramente especificados: el médico tratante y colaboradores más inmediatos en-

---

[76] Artículo 54: «En relación a la obtención y custodia del Expediente Clínico la Comisión Departamental de Auditoría Médica – CDAME acudirá al establecimiento de salud de donde procede el caso que motivo la solicitud de la Auditoría Médica y con una credencial específica conferida por el Director del SEDES, obtendrá a través del Director del establecimiento, el expediente clínico completo y original del paciente correspondiente al caso, para su custodia en el SEDES, en tanto dure todo el proceso de auditoría hasta su finalización, con la previsión de dejar en el establecimiento una copia fotostática del expediente clínico, hasta la devolución del original».

[77] Artículo 55: «Como constancia de la entrega y recepción del Expediente Clínico se llena el acta correspondiente del Formulario N.º 1 con copias debidamente firmadas, tanto para el Director del establecimiento como para la Comisión Departamental de Auditoría Médica».

cargados de seguir evoluciones y prescripciones, y la enfermera que tiene la misión de cumplir las prescripciones (artículo 21).

5.1.7.1 **Anotaciones subjetivas**

En la práctica, cuando se solicita copia de los datos que figuran en la historia clínica por parte del paciente o de las personas que legítimamente pueden acceder a los mismos, podría interpretarse que el profesional puede seleccionar los datos que va a facilitar, algo que resulta enormemente peligroso para la protección de los derechos del paciente, y no simplemente los de contenido patrimonial, dado que una actuación obstrusiva del médico puede suponer que otros profesionales no puedan actuar adecuadamente respecto del enfermo (Rodríguez López, 2004).

Sobre este particular es conveniente precisar que se han manejado dos órdenes diversos de ideas. Un sector que defendió la opción de establecer el derecho del límite de acceso del paciente a las anotaciones subjetivas del facultativo, en base a que dicho acceso podría provocar en algunos casos más perjuicios que beneficios en la salud del paciente (en la anotación realizada por el facultativo en la que se indica que el paciente tiene un mal pronóstico o que se espera un desenlace fatal), incluso se argumentó que podrían existir para el enfermo dificultades de comprensión exacta del contenido de la historia originadas por el desconocimiento de la terminología científica, lo que podría conducir a errores de interpretación; y concluían los seguidores de esta teoría que si no se reconociesen limitaciones al derecho del paciente para acceder a su historia clínica, existiría una resistencia por parte de los profesionales a incluir las anotaciones subjetivas en las historias clínicas. De otro lado, estaban quienes defendían el acceso absoluto e indiscriminado del paciente a su historia clínica (Méjica García y Díez Rodríguez, 2006).

Como es lógico, se presentan algunas dificultades como definir qué son las anotaciones subjetivas y quién determina que lo son y por lo tanto asume la responsabilidad de su protección. Junto a estas dos limitaciones expresamente recogidas en la Ley 41/2002 debe mencionarse igualmente el interés terapéutico del propio paciente.

Si mediaran justas razones por las que fuese necesario o aconsejable retirar datos de una historia clínica, bien por haber sido facilitadas por terceros o por formar parte de la labor deductiva del facultativo, la eliminación o supresión de los mismos en ningún caso podría dejarse al mero arbitrio del facultativo que prestó la asistencia sanitaria, sino que sería necesaria la intervención del Comité de Ética Asistencial, o en su defecto, de la Dirección Médica del Centro sanitario y desde luego basarse en criterios de objetividad e imparcialidad y nunca con el propósito de salvaguardar las eventuales responsabilidades del facultativo (Méjica García y Díez Rodríguez, 2006).

5.1.7.2 **Paciente fallecido**

El artículo 18.4 de la Ley 41/2002 de España señala que los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo prohibiese expresamente y así se acredite. En cualquier caso, el acceso de un tercero a la historia clínica, motivado por un riesgo para su salud, se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido, ni las anotaciones subjetivas de los profesionales, ni que perjudiquen a terceros.

El acceso de un tercero a la historia clínica del paciente, motivado por un riesgo para su salud, se limitará a los datos pertinentes. Especial relevancia tiene este apartado en el caso de las enfermedades infecto-contagiosas, sobre todo la falta de concreción de la información que se debe facilitar a este tercero y el alcance de la expresión «datos pertinentes». Otra cuestión que se puede suscitar es la de si el tercero que pide el acceso a la historia clínica del fallecido por razones de riesgo para su salud, necesariamente tiene que ser un familiar o persona vinculada al paciente por razones familiares o de hecho, o si se puede referir también a otro tipo de tercero, por ejemplo, en las enfermedades de transmisión sexual –VIH o VHC– si el acceso puede otorgarse a este tercero(a) que ha mantenido esporádicamente alguna relación íntima con el fallecido (Méjica García y Díez Rodríguez, 2006).

Cuando es la aseguradora la que solicita los datos de la historia clínica de un fallecido, ésta sólo tiene derecho a conocer los datos del certificado de defunción, y si solicita más información de la que se

menciona en el mismo deberá solicitar la autorización de acceso a los titulares de esta información que son los herederos del paciente (Álvarez – Cienfuegos, 2000).

5.1.7.3 **Fines judiciales**

El acceso a la historia clínica para el cumplimiento de los fines antes expuestos obliga a disociar los datos, de forma tal que se preserven los datos de identificación personal del paciente separados de los de carácter asistencial, de manera que quede asegurado el anonimato y ello salvo que el propio paciente haya prestado expresamente su consentimiento para no separarlos. Se exceptúa de esta disociación de datos los supuestos de investigación de la autoridad judicial, en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los Órganos Judiciales en el proceso correspondiente (Rodríguez López, 2004).

La cesión de la historia clínica a los órganos judiciales está vinculada a otro derecho, el de la tutela efectiva que es también un derecho fundamental y que está al mismo nivel que el derecho a la intimidad y el derecho a la protección de datos personales. De hecho el propio conocimiento de los tribunales es garantía de todos los derechos e intereses legítimos. La cesión de la historia clínica por parte de los órganos judiciales no plantea ningún inconveniente cuando se cuenta con la autorización del paciente. En el caso de que éste no la dé, el médico ha invocado en ocasiones secreto profesional. El problema es que este secreto profesional está en contradicción, no con la voluntad del órgano judicial, sino con el derecho a la tutela judicial efectiva de otro ciudadano. Es decir, no se trata de un conflicto entre el derecho a la intimidad y a la protección de datos de carácter personal, y la competencia de los Tribunales, sino entre esos derechos y el derecho que tienen las personas a obtener una tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que en ningún caso, pueda producirse indefensión. Este conflicto de derechos debe ser resuelto por el juez, no por el médico. (Troncoso Reinaga, 2006).

Es decir, no le corresponde al médico valorar la solicitud judicial y la intimidad del paciente y decidir en consecuencia, la tutela de los

derechos y la resolución de los conflictos está en los sistemas políticos español y boliviano en manos de los jueces, única instancia independiente, inamovible, responsable y sometida únicamente al imperio de la Ley.

La Ley 41/2002 de España y la Ley 3131 de Bolivia es consciente de la legitimidad de la cesión de historias clínicas a los efectos judiciales. Los jueces deben limitar su petición de acceso a la historia clínica a los datos imprescindibles y los médicos, vista a veces la ambigüedad de algunas peticiones judiciales, tienen que aplicar el «principio de proporcionalidad», dando información que consideren necesaria en cada caso, y pidiendo aclaraciones si resulta necesario a los propios órganos judiciales. A la hora de la cesión de datos a los órganos judiciales, es conveniente diferenciar también las distintas jurisdicciones en virtud de los bienes jurídicos tutelables. Así, tiene una primacía clara el orden penal sobre el orden civil. El juez debe ser cuidadoso a la hora de pedir información de la historia clínica (Troncoso Reinaga, 2006).

Con relación al acceso a la historia clínica para el cumplimiento de fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, la Ley 41/2002 constituye la normativa supletoria puesto que, en tales materias, se aplican como normas especiales la LOPD, la Ley General de Sanidad y las demás normas de aplicación en cada caso.

5.1.7.4 **Menores de edad**

Los menores son titulares de derechos fundamentales que también ejercen el ámbito sanitario. La Carta Europea de los Niños Hospitalizados aprobada mediante Resolución del Parlamento Europeo de fecha 13 de mayo de 1986 ha reconocido también un conjunto de derechos específicos de los menores en el ámbito sanitario. Entre estos derechos, el menor tiene también un derecho a la intimidad y a la protección de sus datos personales, que se extiende no sólo al derecho de acceso a la historia clínica sino también a la garantía de su confidencialidad frente a accesos indebidos de ésta. La Ley 41/2002 regula específicamente el consentimiento por representación para los pacientes menores de edad estableciendo esta posibilidad cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de

comprender el alcance de la intervención. En pacientes con dieciséis años cumplidos o emancipados hay que señalar que los padres deben poder acceder a la historia clínica de los menores cuando se trate de temas de salud importantes, sin perjuicio de que su opinión sólo sea tenida en cuenta en caso de actuación de grave riesgo. La capacidad de acceso de los padres a la historia clínica, mientras mantengan la patria potestad, tiene que ser mayor que su capacidad de tomar decisión y no debe limitarse a las actuaciones de grave riesgo. En pacientes que no han cumplido todavía los doce años, estos menores tienen dificultades cognitivas y valorativas para la toma de decisiones. El consentimiento para el tratamiento médico lo prestan sus representantes legales teniendo estos el derecho de acceso a la historia clínica y a los datos sanitarios, no teniendo ningún derecho en este ámbito el menor de edad (Troncoso Reinaga, 2006).

Si la regla general es reconocer una importante capacidad de obrar en derecho a partir de los catorce años, la Ley 41/2002 ha elevado esta edad a los dieciséis años exista o no emancipación. Entre los doce y dieciséis años es necesario escuchar la opinión del menor, pero el consentimiento les corresponde a sus padres. En todo caso la Ley introduce la apreciación sobre la capacidad intelectual y emocional del menor para comprender el alcance de una intervención, como criterio importante para la solicitud del consentimiento por representación y por tanto, para el ejercicio de los derechos de acceso a la historia clínica y a los datos sanitarios.

5.1.7.5 Fines epidemiológicos de salud pública, investigación o docencia

Los fines epidemiológicos tiene como objetivo preservar la sanidad colectiva de los ciudadanos; y los de investigación y docencia, el avance de la ciencia, lo que redunda también en beneficio común. En estos supuestos, la utilización de los datos, toda vez que la Ley 41/2002 requiere, con buen criterio, la separación de los datos identificativos y los datos asistenciales, de manera que puedan garantizarse el anonimato del paciente. Lo que establece el apartado del artículo 16.3 de la Ley cuando señala que «el acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso».

En Bolivia el artículo 7 (Finalidades) de la Norma Técnica para el Expediente Clínico establece los múltiples usos y aplicaciones del expediente clínico:

— *Docencia:* por constituirse en un instrumento de enseñanza para la capacitación de recursos humanos en salud (artículo 7.2).

— *Investigación:* por contener información que proporciona datos para la programación, control y evaluación epidemiológica de enfermedades prevalentes, o para el estudio e información de condiciones patológicas especiales o infrecuentes (artículo 7.3).

5.1.7.6 Personal sanitario que ejerce las funciones de inspección o evaluación, acreditación y planificación

La actividad de los inspectores médicos comprende actos de genuino ejercicio de la actividad médica, así, su seguimiento de las altas y bajas médicas, control de las hospitalizaciones, participación en los Equipos de Valoración de Incapacidades, revisiones, dictámenes clínicos, laborales, etc., constituyen un conjunto de intervenciones reservadas a la profesión médica, por lo que el acceso a la historia clínica de los pacientes en el ejercicio de sus funciones no implican en absoluto revelación de secretos por razones funciones y también legales. En esta línea de criterio, el Auto de la Audiencia Provincial de Segovia de España de fecha 19 de diciembre de 2000 declara que el médico debe facilitar a la inspección el acceso a las historias clínicas íntegras por gozar de evidente cobertura normativa (Méjica García y Díez Rodríguez, 2006).

El personal sanitario que ejerce funciones de inspección, evaluación, acreditación y planificación también tiene acceso a las historias clínicas en el cumplimiento de las funciones de comprobación de calidad de la asistencia (artículo 31.1 Ley General de Sanidad), el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes o la propia Administración (artículo 16.5 de la Ley 41/2002). Por último, se faculta a las Comunidades Autónomas para que regulen el procedimiento para que quede constancia del acceso a la historia clínica.

En Bolivia la Norma Técnica para el Expediente Clínico establece en el artículo 7 (Finalidades) los múltiples usos y aplicaciones del expediente clínico:

— *Gestión y planificación de recursos:* por constituirse en el registro único de las actividades asistenciales realizadas por los miembros del equipo de salud que participan en la prestación de servicios a los pacientes y los recursos que emplean (artículo 7.4).
— *Control de calidad asistencia:* porque a través del expediente clínico se puede verificar el cumplimiento a normas y protocolos que se enmarcan en la calidad de atención (artículo 7.8).

5.1.7.7 **Fines administrativos y de gestión**

Por lo que se refiere al personal de administración y gestión de los centros sanitarios, los mismos solo pueden acceder a los datos de la historia clínica relacionados con sus propias funciones, tal como declara la Ley 41/2002.

La Ley 41/2002 exige también la disociación o separación de los datos clínicos asistenciales de los propios datos de carácter administrativo y de gestión, indicando que el personal de administración solo podrá acceder a éstos últimos (Méjica García y Díez Rodríguez, 2006).

En Bolivia la Norma Técnica para el Expediente Clínico establece en el artículo 7.6 que puede ser utilizada por la «Administración, porque aporta datos imprescindibles para el manejo administrativo financiero y no financiero de las instituciones, los subsectores prestadores de servicios y el propio Sistema de Salud».

5.1.7.8 **Acceso a la historia clínica electrónica y seguridad**

Es esencial que en todo caso quede garantizada la seguridad, cualquiera que sea el soporte material en que se contenga la historia clínica; expresamente, la Ley 41/2002 prevé que las historias deberán ser archivadas por el centro sanitario, cualquiera que sea su soporte (papel, audiovisual o informático). El desarrollo de las tecnologías digitales ha facilitado que éstas actualmente se hallen al alcance, no sólo de los grandes centros hospitalarios o del sistema sanitario público, sino también de todos los profesionales de la salud, por lo que se apuesta por un modelo de tratamiento informático de las historias clínicas (frente al soporte papel), por el establecimiento de una histo-

ria única para cada paciente de un mismo centro sanitario y por la historia clínica compartida entre los profesionales sanitarios.

La Ley 44/2003 de Ordenación de las Profesiones Sanitarias de 21 de noviembre establece, al regular los principios generales del ejercicio de las profesiones sanitarias, que existirá una formalización escrita del trabajo de los profesionales sanitarios, reflejado en una historia clínica que deberá ser común para cada centro y única para cada paciente atendido por él. Además, dispone la ley, que la historia clínica tenderá a ser soportada en medios electrónicos y a ser compartida entre profesionales, centros y niveles asistenciales.

El uso de la tecnología informática es de gran utilidad para establecer niveles de acceso autorizados en las historias clínicas electrónicas y controles de seguridad basados en el uso de certificados digitales y firmas electrónicas.

El personal que se ocupa de las funciones de administración y gestión de los centros sanitarios y de las consultas de los profesionales sanitarios tiene un acceso a la historia clínica limitado a aquellos datos que sean necesarios para desarrollar sus funciones de administración o gestión de actividad sanitaria, teniendo excluido el acceso a cualquier otro dato personal y prohibido un uso distinto del que le corresponda en el ejercicio de sus funciones (Martí y Pidevall, 2004).

En estos casos adquiere especial importancia la necesidad de que los centros se doten de los mecanismos físicos o informáticos dirigidos a evitar que personas no legitimadas accedan a datos íntimos, siendo frecuente la articulación de distintos niveles de autorización de acceso a las bases de datos en los sistemas informáticos, mediante la atribución al personal autorizado de claves de acceso *(password)* o firmas electrónicas que garanticen que no se produce una extralimitación en el acceso y que eventualmente pueda acreditarse la trazabilidad de ese acceso.

5.1.8 QUIÉN DEBE REALIZAR LA HISTORIA CLÍNICA

La competencia para la creación y actualización de la historia clínica es el facultativo que realiza la asistencia sanitaria al paciente, como una obligación o contraprestación derivada del derecho del pa-

ciente a que quede constancia por escrito de todo su proceso asistencial (Méjica García y Díez Rodríguez, 2006).

Así, el artículo 15.3 de la Ley 41/2002 señala que «la cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será responsabilidad de los profesionales que intervengan en ella».

No puede desconocerse que, además del médico, existen otros profesionales que participan en la redacción de la historia clínica, al menos en parte de ella, como es el caso de las Hojas de enfermería; es lo que en términos legales, el artículo 15 de la Ley 41/2002 denomina como «aplicación terapéutica de enfermería», que deberá actuarse siempre bajo la dirección, órdenes e indicaciones dados por el personal médico facultativo.

En Bolivia la Norma Técnica para el manejo del Expediente Clínico establece sobre la historia clínica que el responsable para su elaboración, dentro de las 8 horas de transcurrida la hospitalización, es el médico tratante. En los hospitales de enseñanza, la historia clínica puede ser elaborada por delegación del médico tratante al médico residente de la unidad o servicio donde se hospitalizo al paciente, o por el estudiante de último año que se encuentra cumpliendo su internado rotatorio, bajo la supervisión y revisión del médico de planta, quién necesariamente dará su conformidad, estampando su nombre, sello y firma al pie del documento (artículo 12.4).

Los documentos de enfermería están conformados por las notas de evolución de enfermería y el registro de tratamientos. Las notas de evolución de enfermería son las notas que escribe enfermería con relación al estado del paciente, su evolución y las constataciones que haga respecto a las intercurrencias o complicaciones que pudiesen presentarse. Estas notas deben ser cuidadosamente elaboradas y llevar firma y sello de le enfermera responsable de su elaboración (artículo 12.13.1). Las notas de registro de tratamientos de enfermería las escribe la enfermera en cumplimiento a las prescripciones u órdenes médicas. Revisten especial importancia, porque constituyen la constancia del cumplimiento de las prescripciones, tal cual fueron escritas y firmadas por el médico (artículo 12.13.2)

En esencia, se concluye que la historia clínica es un «documento médico», redactado fundamentalmente en interés de la salud del paciente, de evolución diaria, que debe contener anotaciones continuas,

ha de ser legible y no debe contener siglas o abreviaturas no aceptadas, también debe contener fecha y firma.

5.1.9 LA CUESTIÓN DEL VALOR PROBATORIO DE LA HISTORIA CLÍNICA ELECTRÓNICA

La Ley 59/2003 de Firma Electrónica de fecha 19 de diciembre de 2003 de España establece la distinción entre el concepto de firma electrónica, firma electrónica avanzada y firma electrónica reconocida, en los siguientes términos:

1. «*La firma electrónica* es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

2. *La firma electrónica avanzada* es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

3. Se considera *firma electrónica reconocida* la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

4. La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel».

En cuanto a su valor probatorio, el apartado 8 del mismo precepto señala que: «El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida, con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumplen todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan

firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326[78] de la Ley de Enjuiciamiento Civil».

Méjica García y Díez Rodríguez (2006:228) entienden que la historia clínica informatizada será válida como elemento probatorio en un proceso, sin perjuicio de que las otras partes puedan aportar dictámenes y otros medios probatorios que cuestionen su autenticidad y exactitud y además, deberá ser valorada por el Juez según las reglas de la sana crítica y de la experiencia, por lo que convendría instalar medidas de seguridad en los ordenadores de los facultativos que permitieran identificar al facultativo, realizar copias de seguridad *(back up)* e instalar sistemas informáticos de rastreo *(tracking)* en los que consten entradas en el sistema como medio de garantizar la autenticidad de los documentos.

5.2 SECRETO MÉDICO

Hoy día, el secreto profesional ya no se conceptúa solamente y en primer lugar como un deber profesional, sino como un derecho ciudadano. Por tanto, se trata de uno de los llamados derechos-deberes, ya que es un derecho que genera en los profesionales un deber específico, hay un deber general de respeto a la intimidad de todos los seres humanos y hay otro específico y cualificado de los profesionales, ya sean abogados, procuradores, médicos, etc., todos ellos tienen una obligación específica y cualificada de guarda del secreto, pero los profesionales sanitarios, ya desde el Código Penal francés del año 1810, artículo 378, estaban obligados a denunciar algunas circunstancias a

---

[78] Artículo 326 de la Ley 1/2000 de Enjuiciamiento Civil de España «2. Cuando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto. Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el Tribunal lo valorará conforme a las reglas de la sana crítica. 3. Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a los establecido en el artículo 3 de la Ley de Firma Electrónica».

la autoridad. En este Código se diferenció el secreto médico del secreto profesional propio de los sacerdotes, jueces, procuradores o abogados; el secreto médico comienza a configurarse como peculiar y especial (Sánchez Carazo, 2000).

El secreto médico tiene su fundamento en la relación de confianza que debe existir entre el médico y el paciente, esta confianza debe ser respetada por el profesional de la medicina con el objeto no sólo de proteger la integridad física del paciente, en cuanto al anonimato de sus enfermedades, sino también de proteger la integridad de la persona, pues una revelación indebida de sus padecimientos puede acarrear un perjuicio moral que es susceptible de incriminación.

Como señala Sánchez Carazo (2000:73) «el paciente desnuda su cuerpo y, en muchos casos su alma, ante el médico, éste le trata en los momentos más vulnerables de su vida: nacimiento, enfermedad, dolor, impotencia, muerte. El médico, a diferencia del abogado o del sacerdote, llega a conocer incluso cuestiones que al propio sujeto no le gustaría mostrar, pero el facultativo, para poder curar o aliviar el dolor, ha de conocer profundamente al enfermo».

López Gomón y Gisbert Calabuig (1998:76) definen el secreto médico como: «la obligación debida a las confidencias que el médico recibe de sus clientes, como médico, hechas con vistas a obtener cualquier servicio de los que comporte la profesión».

Según Zubiri Vidal (2001:11) citado por De Miguel (2002): «es el que nace del ejercicio de la profesión médica, y es la suma del secreto natural y del confiado, es natural por cuanto interviene algo cuya revelación redundaría en perjuicio del cliente, y también, por el mero hecho de ser confiado, es el que otorga a una persona con la condición previa, explícita o implícita, de no revelarlo a nadie, surgiendo un contrato bilateral que refuerza una obligación de secreto que se revela como tal por su propia naturaleza».

En España los Códigos Deontológicos dan gran importancia al secreto profesional, entre ellos hay que destacar el Código de Ética y Deontología Médica Española, aprobado el 31 de marzo de 1990 por la Asamblea General de la Organización Médica Colegial, o también llamado nuevo Código de Ética y Deontología Médica, que contiene un conjunto de principios y reglas éticas que deben inspirar la conducta profesional del médico y obliga a todos los médicos en el ejer-

cicio de su profesión, cualquiera que sea la modalidad en que la practiquen.

Defiende que el médico actuará siempre con corrección, respetando con delicadeza la intimidad de su paciente; el capítulo IV de dicho Código está dedicado al secreto profesional. La Asamblea del Consejo General de Colegios Médicos aprobó el Código Deontológico el 25 de septiembre de 1999; en el apartado correspondiente al secreto profesional trata la problemática que se produce con la informatización de los datos de carácter personal relativos a la salud, establece que la informatización de los datos sanitarios no ha de poner en peligro la intimidad de los pacientes, e incluso afirma que estos no pueden estar conectados a redes informáticas.

También en los Códigos Deontológicos del resto de profesionales sanitarios se ha defendido la intimidad del paciente, por ejemplo, el Código Deontológico del Psicólogo, promulgado por el Colegio Oficial de Psicólogos, o el Código Deontológico de la Enfermería Española. Como puede observarse, existe una extensa reglamentación deontológica profesional de lo que, en principio, es una de las cualidades fundamentales de la profesión médica: el derecho a no revelar nada que afecte a la intimidad de un paciente que ha comunicado, confiado sus datos al médico. Incluso uno de los motivos de infracción grave es el incumplimiento por parte del personal sanitario del deber de garantizar la confidencialidad y la intimidad de los pacientes en la tramitación de las recetas y órdenes médicas (Criado del Río, 1999).

En la actualidad la medicina es ejercida por equipos que necesitan compartir la información para poder dar al enfermo una atención de calidad. El sujeto que ingresa en un centro sanitario tiene relación con múltiples profesionales, sus datos se almacenan en grandes archivos y en ordenadores conectados con diversas bases de datos y múltiples profesionales, incluso en algún caso pudieran estar conectados a Internet, por lo que profesionales de otros centros u otros países pueden tener acceso a los datos sanitarios de una persona, con el peligro que entraña la posibilidad de acceso a dicha información por personas no autorizadas.

Señala Sánchez Carazo (2000:74) que «la medicina en equipo obliga a replantear los mecanismos jurídicos de tutela de los derechos de los pacientes y, en especial, de su derecho a la intimidad». Cuando

una persona entra en contacto con la sanidad también entra en contacto con otras muchas personas, telefonistas, secretarias, personal de seguridad, entre otras, y es importante dejar muy claro que todos ellos están sujetos al secreto y que todos los trabajadores que revelen hechos o datos personales conocidos por razón de su oficio están sujetos a las penas correspondientes.

El Código Penal español (Ley 10/1995 de 23 de noviembre), defiende de forma novedosa la intimidad dedicando a ello todo el Título X «De los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», dicho Título está divido en dos capítulos, el primero de ellos está dedicado a los delitos contra la violación de la intimidad de las personas y el segundo contra la violación de la intimidad del domicilio.

Lo que la ley castiga en el secreto es otra cosa distinta a su conocimiento, y consiste precisamente en la violación de la prohibición de la comunicación a un tercero; es decir, la divulgación del contenido del secreto, implica pues, una obligación negativa, que es contrapunto al deber positivo de discreción por parte del profesional, en busca de la protección del bien jurídico consistente en la intimidad del enfermo. Con independencia de las repercusiones posteriores que pueda implicar la relación profesional, en general, y la del médico con su paciente, en particular, el punto de partida se halla en la necesidad que este último tiene de acudir al primero a la espera de un consejo profesional que responda a un problema que él mismo no puede resolver (De Miguel, 2002).

A pesar de que la legislación civil, penal y los Códigos Deontológicos insisten en el secreto médico, resulta que en algunos casos los facultativos se pueden ver obligados a revelar datos de sus pacientes, es más, en lo que respecta al secreto profesional médico, en el proceso penal hay que indicar que la Ley de Enjuiciamiento Criminal de 14 de septiembre de 1882 no incluye a los profesionales de la medicina entre las personas que quedan dispensadas de la obligación de declarar, y tampoco los médicos facultativos figuran entre las personas que no podrán ser obligadas a comparecer como testigos. Por otro lado, la Ley de Enjuiciamiento Criminal establece una obligación general de denunciar los hechos delictivos que se conozcan en ocasión del cargo, profesión u oficio que se desempeñe; de este régimen general sólo

quedan excluidos los abogados y procuradores, los eclesiásticos y ministros de culto.

Uno de los principales motivos por los que se tendrán que dar a conocer ciertas confidencias es el de la defensa del interés general. Este es el caso de la declaración de las enfermedades reguladas como de declaración obligatoria en las que hay un deber explícito de comunicar a determinadas personas y organismos la existencia de dichas enfermedades. En éste ámbito existe una frecuente contradicción entre los principios de intimidad y de salud pública que se suele resolver a favor de la intervención pública garante del interés general establecida en la legislación sanitaria, pero con las limitaciones y garantías de la LOPD, relativas a la adecuación y pertinencia de los datos solicitados en relación con el fin buscado, el cumplimiento del deber de secreto de las personas que tienen acceso a los datos, al igual que la adopción de las medidas técnicas y organizativas que impidan el acceso indebido a los mismos, y en último término, la garantía de los derechos del afectado (Tomas-Valiente *et al.*, 2006).

Sánchez Carazo (2000) señala que la obligación de guardar secreto cesaría cuando se diese alguna de las siguientes situaciones:

— La persona interesada permite la relevación.

— La materia deja de ser secreta.

— La violación del secreto evitará un grave daño al bien común o a una tercera persona.

Los problemas más importantes que se plantean a las posibles excepciones al secreto, a los deberes de confidencialidad, se refieren al tercer punto; antes de tomar una decisión hay que tener en cuenta que cada posible excepción necesita ser examinada y justificada cuidadosamente. La presunción debe estar a favor del secreto, porque las consecuencias de la violación pueden ser muy graves para las personas interesadas y para la sociedad misma. Señala Sánchez Carazo (2000:105) que «lo que quiere es suscitar la reflexión, plantear el problema real al que se enfrenta el médico cuando se encuentra en una situación de conflicto de valores: el secreto profesional y el derecho a la intimidad, derecho de autonomía del paciente versus el derecho de terceros o el bien común».

Ocurre con gran frecuencia que el Juzgado o Tribunal se dirige al facultativo para reclamarle el historial clínico de un paciente o para

prestar declaración sobre algún dato o hecho de los que haya podido conocer a consecuencia de su ejercicio profesional. Tradicionalmente, la doctrina viene haciendo una distinción en atención al tipo de procedimiento del que se trate, así se debe entender que no es lo mismo la reclamación del historial del paciente en un procedimiento civil o penal en el que está enjuiciando la correcta actuación del facultativo, que la reclamación del referido historial en procedimientos con distinta finalidad, en los procedimientos civiles de separación o divorcio, o en procedimientos laborales por despido, supuestos éstos donde se entiende que la petición judicial debe estar claramente motivada y fundamentada, y el acceso a la información debe ser mucho más restringido que el primer supuesto, siendo además aconsejable que el facultativo advierta al juzgador de su deber de secreto profesional, sometiendo ante él tal circunstancia (Méjica García y Díez Rodríguez, 2006).

El deber del secreto profesional médico, no sólo afecta al paciente en vida sino que se prolonga aun después de su muerte, pues éste una vez muerto posee aún derechos personalísimos, como el derecho a su dignidad, a la buena reputación y a no ser difamado. Una situación que se da con frecuencia en la práctica es la solicitud de datos clínicos del paciente ya fallecido. La muerte del paciente y sus causas se constatan en el certificado de defunción que se realiza cuando ésta es natural y se conocen sus causas. Las muertes violentas o sospechosas de criminalidad se ponen en conocimiento de la justicia por medio de un parte tras el que se pondrán en marcha las diligencias correspondientes. El médico que asistió al paciente fallecido únicamente debe seguir este procedimiento e informar a los familiares o personas que designó para ello el paciente de los datos del informe de alta, del certificado de defunción y de los resultados de la autopsia clínica, para cuya realización es necesaria también la autorización de los familiares (Criado del Río, 1999).

Especial significación tiene el secreto médico ante los requerimientos realizados por los Colegios profesionales a los facultativos con la finalidad de obtener información sobre quejas planteadas por los pacientes, y en especial la conjugación de este derecho con el deber de colaboración y de atención a los requerimientos colegiales que vienen descritos en la gran mayoría de los Estatutos de las referidas corporaciones. No obstante, se entiende que con carácter general no se podrá oponer ante cualquier requerimiento colegial la alegación de vulnera-

ción de la confidencialidad del datos sanitario, ya que el secreto médico es un deber jurídico impuesto al facultativo pero nunca un privilegio de éste, por lo que será preciso analizar cada caso en concreto y el conjunto de sus circunstancias para poder determinar si existe o no la referida vulneración; el supuesto contrario, desde luego, limitaría e impediría la clásica función de control deontológico de la profesión atribuida a los Colegios Profesionales (Méjica García y Díez Rodríguez, 2006).

Especial consideración merecen los supuestos de extinción o rescisión de contratos administrativos de gestión de servicios sanitarios y la sustitución de los equipos sanitarios derivada de una nueva contratación, y todo ello en relación con la información sanitaria de que disponía el equipo anterior. La transmisión de la información asistencial no vulnera por sí mismo e derecho a la intimidad de los pacientes, y se considera necesaria para garantizar la continuidad y efectividad del servicio, todo ello sin perjuicio de que si la Administración hiciera en un futuro un mal uso de la misma, se genere responsabilidad respecto de meras hipótesis o futuras conjeturas más o menos verosímiles, como tiene declarado la jurisprudencia constitucional española.

Una situación de conflictividad es la que genera la revelación a parientes o personas íntimamente ligadas al paciente de seropositividad del mismo. En opinión de Méjica García y Díez Rodríguez (2006:130-131) «el problema se centra en determinar la prevalencia de los derechos en juego. Y entendemos que cuando existe un más que evidente riesgo de contagio para terceras personas, éstas pueden ser informadas, siempre y cuando el enfermo no lo haya realizado con anterioridad, porque, aun siendo esencial en la relación sanitaria el principio de secreto y confidencialidad, éste no tiene carácter absoluto y admite limitaciones en interés de la colectividad y de terceros».

El Capítulo VII del Código de Ética y Deontología Médica establece que el *secreto médico* es el compromiso que le prohíbe divulgar o permitir que se conozca libremente la información que obtiene sobre la salud y la vida de una persona o de la familia de ésta. El secreto profesional, instituido en el interés de los pacientes, se impone a todo médico en las condiciones establecidas por la Ley 3131. El secreto cubre todo lo que llega al conocimiento del médico en el ejercicio de su profesión, es decir no solamente lo que le ha sido confiado, sino también lo que él ha visto, escuchado o comprendido (artículo 69).

La obligación de respetar el secreto médico se mantiene aún después que haya cesado la prestación de sus servicios, así como con posterioridad a la muerte del paciente (artículo 70).

Las situaciones de excepción que exime al médico de guardar el secreto profesional son las siguientes:

1. Mandato de la ley.
2. Autorización expresa del paciente.
3. Función de médico forense o legista.
4. Denuncia obligada de enfermedades infecto-contagiosas ante autoridades competentes.
5. Petición de representantes legales de menores de edad. En esta circunstancia, si el interés del menor lo exige, podrá abstenerse de dicha revelación.
6. Cuando se trate de salvar la vida y el honor de las personas.
7. Para impedir la condena de un inocente.
8. Salvaguarda de responsabilidad de terceros en proceso judicial.
9. Defensa propia ante imputación de daños causados en el ejercicio de la profesión (artículo 71).

El secreto profesional debe mantenerse por todos los médicos que intervengan en el caso clínico (artículo 72). El secreto profesional incluye el nombre del paciente y de la institución (artículo 73).

El Código Penal boliviano aprobado mediante Decreto Ley 10426 de fecha 23 de agosto de 1072 elevado al rango de Ley 1768 en fecha 10 de marzo de 1997 establece en el artículo 302 (Revelación de secreto profesional): «El que teniendo conocimiento de secretos en virtud de su estado, ministerio, profesión, empleo, oficio, arte o comisión, los revelare sin justa causa, o los usare en beneficio propio o ajeno, si de ello se siguiere algún perjuicio, será sancionado con privación de libertad de tres meses a un año y multa de treinta a cien días».

El revelar el secreto profesional es considerado como delito siempre y cuando la revelación tenga por finalidad el ocasionar un perjuicio de cualquier naturaleza al titular de la información que se pretende proteger; por ejemplo, un médico acerca de una enfermedad delicada. La salvedad se presenta, cuando existe un interés superior para vencer el secreto profesional. Por ejemplo, cuando el médico

sabe y le consta que el paciente es portador de VIH – SIDA, y conoce también la voluntad del individuo de no comentar este hecho con su pareja a quien puede sin duda contagiar. El deber en este caso del profesional no será publicitar el hecho, pero si tendrá la obligación de dar toda la información necesaria al portador como también informar a la pareja, con la finalidad de evitar un posible contagio (Valda Daza, 2014).

El Código de Procedimiento Penal boliviano respecto al secreto profesional establece los casos en los cuales esta condición debe respetarse, suspenderse, e inclusive ordenarse se levante la obligación al titular de la información reservada. Artículo 197.º (Deber de abstención). «Las personas deberán abstenerse de declarar sobre los hechos que hayan llegado a su conocimiento en razón de su oficio o profesión y se relacionen a deberes de secreto y reserva legalmente establecidos. Estas personas no podrán negar el testimonio cuando sean liberadas por el interesado del deber de guardar secreto. En caso de ser citadas, deberán comparecer y explicar las razones de su abstención. Si el juez estima que el testigo invoca erróneamente ese deber con respecto a un hecho que no puede estar comprendido en él, ordenará por resolución fundada su declaración».

Para concluir, cabe señalar que el derecho a la intimidad personal y a la privacidad ha sido, y aún es, un derecho en algunos casos ignorado y en otros mal ponderado, ya sea porque los profesionales incumplen el deber de no revelar o porque nuestra sociedad es poco celosa a la hora de exigir que se respete su derecho a la privacidad.

CAPÍTULO VI
LA HISTORIA CLÍNICA ELECTRÓNICA

6.1 HISTORIA CLÍNICA ELECTRÓNICA

La introducción de las tecnologías de la información y de las comunicaciones (TIC) en los centros sanitarios se hizo a través de equipos de diagnóstico médico y de los servicios de gestión económico-financiera, como la contabilidad o la facturación y la nómina de su personal. Más tarde se desarrollaron aplicaciones para los servicios clínico-administrativos, como la gestión de camas, la cita previa de consultas externas, o la gestión del archivo de historias clínicas, a estas aplicaciones siguieron los programas de codificación de los sistemas de clasificación de pacientes. El siguiente paso ha sido el de la informatización de la historia clínica, que supone introducir las TIC en el núcleo de la actividad sanitaria, como es el registro de relación entre el paciente y los médicos y demás profesionales sanitarios que le atienden (Carnicero Giménez, 2004).

La irrupción de las TIC como un instrumento clínico se produce en un contexto de cambios en la sociedad, tanto del mundo como en España y en Bolivia, que por un lado obligan a los servicios de salud a establecer estrategias para adaptarse a esos cambios, y por otro suponen una oportunidad para aprovechar las ventajas de la historia clínica electrónica en la mejora de la práctica clínica.

No existe ningún impedimento legal para que la información recogida en la historia clínica se informatice, es más, la historia clínica electrónica tiene el mismo valor jurídico que la historia clínica en soporte papel, al informatizar dicha información, se deberán tener en cuenta tanto el artículo 18.4 de la Constitución Española, que establece la limitación al uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, como la LOPD y el Reglamento de desarrollo de la LOPD (Jañez Ramos *et al*., 2002).

Como establece Carnicero Giménez (2004:272) el concepto de historia clínica cambia con la informatización «de ser un registro del proceso o procesos de un paciente vinculado a un profesional o a un

centro sanitario, pasa a ser un registro de todos los antecedentes de salud de una persona que forma parte de un sistema integrado de información».

En un reporte sobre la historia clínica electrónica presentado por el *Institute of Medicine* (IOM) de los Estados Unidos en los años noventa, la definía como: «…aquella que reside en un sistema electrónico específicamente diseñado para recolectar, almacenar, manipular y dar soporte a los usuarios en cuanto a proveer accesibilidad a datos seguros y completos, alertas, recordatorios y sistemas clínicos de soporte para la toma de decisiones, brindando información clínica importante para el cuidado de los pacientes…».

En una revisión realizada a dicho reporte, el *Institute of Medicine* (IOM) amplió la definición de historia clínica electrónica:

— Colección longitudinal de información electrónica sobre la salud de las personas donde la información sobre salud es definida como información pertinente a la salud de un individuo, o la información de los cuidados de salud provistos a un individuo, por medio de cualquier miembro del equipo de salud.

— Tiene la posibilidad de dar acceso electrónico inmediato a la información de salud personal o poblacional solo a los usuarios autorizados.

— Provee las bases de conocimiento y sistemas de soporte para la toma de decisiones que mejoren la calidad, seguridad y eficiencia de la atención de los pacientes.

— Tiene el objetivo primordial de dar soporte para la eficiencia de los procesos de cuidados de salud.

Representa un conjunto de sistemas que deben estar altamente integrados y que requieren una significativa inversión de tiempo, dinero, cambio de procesos y reingeniería del factor humano (González y Luna, 2012).

La nueva historia clínica, se hace accesible en cualquier tiempo y lugar en que se preste la asistencia, integra información de diferentes sistemas y centros sanitarios; utiliza como un instrumento más los sistemas de ayuda a la toma de decisiones y guías de práctica clínica; forma parte del sistema de información del servicio de salud; y es un poderoso instrumento de mejora de la calidad y la eficiencia del sistema sanitario.

El desarrollo de la historia clínica electrónica debe llevarse a cabo teniendo en cuenta las estrategias de los servicios de salud, las ventajas e inconvenientes que presenta la informatización, su coste, el nuevo concepto de información integral de salud, la necesidad de preservar la confidencialidad de esa información así como de asegurar su integridad y disponibilidad (González y Luna, 2012).

La historia clínica electrónica puede y debe ser más segura y confidencial que la historia clínica en papel, además, debe tenerse siempre presente las características que debe tener una buena historia clínica, que como indica Laín Entralgo (1998:763) son: «idoneidad, integridad, claridad, precisión y elegancia».

6.2 ESTRATEGIAS DE LOS SERVICIOS DE SALUD

El sistema sanitario español debe hacer frente durante los próximos años a los cambios que se están produciendo o se han producido ya en el entorno y que se refieren a los ciudadanos que lo financian con sus impuestos, los pacientes a los que atiende, las nuevas tecnologías, las restricciones presupuestarias y las demandas de los profesionales sanitarios (Carnicero Giménez *et al.,* 2002).

La mejora de las condiciones de vida y de la calidad de los servicios hacen que las expectativas de los ciudadanos sobre lo servicios públicos, sobre todo lo relacionado con atención sanitaria aumenten. Los ciudadanos son más conscientes de sus derechos y están más dispuestos a exigirlos. Las disposiciones de la Ley 16/2003 de Cohesión y Calidad del Sistema Nacional de Salud referidas a la garantía de las prestaciones o la Ley Básica 41/2002 reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica son un reflejo de ese sentir.

Los profesionales sanitarios necesitan mayor disponibilidad de tiempo tanto para la asistencia como para el acceso al conocimiento para hacer frente a la mayor demanda de servicios, a las mayores expectativas de calidad de sus pacientes y a la incorporación de las nuevas tecnologías.

La mayor demanda de servicios y de mayor calidad, las nuevas tecnologías y los requerimientos de los profesionales conducen a un mayor gasto sanitario, que además se produce en una situación de

amenaza de recesión económica en la Unión Europea y por lo tanto, con tensiones presupuestarias (Falagán *et al.*, 2003).

Los servicios de salud responden a esta situación con políticas de gestión de la demanda, organización asistencial más flexible, cuya clave es la historia clínica electrónica, y mejor información para la gestión y la toma de decisiones entre otras medidas.

6.3 MODELOS DE HISTORIA CLÍNICA

La historia clínica electrónica, que supone incorporar las tecnologías de la información y de las comunicaciones (TIC) en el núcleo de la actividad sanitaria, tiene como consecuencia que la historia deja de ser un registro de la información generada en la relación entre un paciente y un profesional o un centro sanitario, para formar parte de un sistema integrado de información clínica.

En la presente investigación se utilizará como sinónimos historia clínica informatizada o historia clínica electrónica. A continuación se desarrollan diferentes modelos de historia clínica:

— *Historia clínica:* el registro de los diferentes episodios de cuidados asistenciales, generalmente ligados a algún tipo de institución sanitaria. La historia clínica clásica es un registro cronológico de acontecimientos y datos.

— *Historia de salud:* es un concepto mucho más amplio que el de historia clínica, se puede definir como el registro longitudinal de todos los acontecimientos relativos a la salud de una persona, tanto preventivos como asistenciales, desde el nacimiento, incluso antes, hasta su fallecimiento. Incluye la historia de atención primaria y de todos los episodios concretos de atención especializada, por lo tanto, la historia clínica clásica estaría incluida en la historia de salud.

— *Historia clínica orientada a problemas:* consiste en ordenar y presentar los datos no de forma cronológica, sino agrupados en torno a problemas identificables. La atención especializada se adapta bien al modelo clásico cronológico porque suele tratar episodios concretos de un comienzo a un final claramente identificables. Sin embargo, los datos tienden a ordenarse de acuerdo a su naturaleza y origen, incluso con papel de diferente co-

lor. En atención primaria los episodios que terminan son pocos, casi siempre se tratan problemas de salud que permanecen vigentes a lo largo de la vida del individuo. Por ello la historia orientada a problemas es el modelo más adecuado.

— *Historia clínica orientada a contextos:* es una historia con una orientación al contexto comunitario donde se tendrían en cuenta no sólo los problemas de salud, sino también el contexto biopsicosocial, las creencias, la dinámica familiar y la cultura social. Más que un modelo de historia distinto es una propuesta para tomar en cuenta la relación que existe entre el contexto y los diferentes problemas de salud.

— *Historia de salud electrónica:* los datos de la historia se registran cuando se producen o se tiene conocimiento de ellos, por lo tanto con carácter cronológico. Lo que diferencia unos modelos de otros es la presentación o vista de los datos. Cuando se utiliza el soporte papel, la forma de anotar la información es la misma que aquella en que se desea su presentación, dando lugar al modelo de historia. Las TIC permiten la presentación dinámica de los datos, de acuerdo con cada necesidad, con independencia de cómo estén registrados. La historia de salud está constituida por un conjunto de registros heterogéneos que con soportes clásicos serían posiblemente inmanejables. Las TIC hacen posible la integración de todos esos datos y superar los conceptos clásicos de modelos de historia clínica haciendo viable el paradigma de historia de salud en forma de Historia de Salud Electrónica (HSE) (Carnicero Giménez *et al.*, 2003).

6.4 FUNCIONALIDADES CLAVE QUE UNA HISTORIA CLÍNICA ELECTRÓNICA DEBE CUMPLIR

Para reforzar el progresivo desarrollo de estos sistemas el *Institute of Medicine* (IOM) publicó un nuevo reporte con énfasis en nueve (9) funcionalidades clave que una Historia Clínica Electrónica (HCE) debía cumplir con el fin de mejorar la seguridad del paciente, lograr una prestación de servicios eficaz, facilitar la gestión de enfermedades crónicas y mejorar la eficiencia (Tang, 2003). Dichas funcionalidades contemplan:

1. *Gestión de la información de salud:* Una HCE debe contener información sobre los problemas actuales del paciente y sus antecedentes, sus medicaciones, alergias y gestión de los contactos que tuvo con el centro asistencial. Esto incluye las evoluciones clínicas en texto narrativo (del médico, enfermero, técnico) o a través de plantillas estructuradas.

2. *Manejo de resultados:* Se refiere a la representación de los resultados de laboratorio y otros exámenes complementarios como imágenes, anatomía patológica y otros. Un acceso rápido a la información sobre exámenes complementarios ahorra tiempo y dinero, evita la redundancia y mejora la coordinación del cuidado de la salud.

3. *Manejo de órdenes médicas:* El ingreso de órdenes, ya sean pedidos de estudios de laboratorio u otros servicios auxiliares, o el ingreso de medicación a través de sistemas de ingreso de órdenes, es el primer eslabón para que una HCE deje de ser un sistema pasivo y pase a tener un rol activo en la salud del paciente. El sistema puede contener una base de conocimiento que permita gestionar más eficientemente la información e interactuar con el profesional para colaborar con sus decisiones.

4. *Sistemas de soporte para la toma de decisiones:* Inicialmente, los sistemas de soporte estuvieron en relación directa con los sistemas de manejos de órdenes, apoyando al diagnóstico o al tratamiento a través de alertas o recordatorios sobre potenciales interacciones o problemas. Su utilidad se ha ido ampliando y hoy tienen una amplia variedad de funciones.

5. *Sistemas de comunicación electrónica y conectividad:* Para Recibir información de servicios auxiliares externos y de otros sistemas, la HCE debe permitir comunicarse a través de una mensajería estándar y una terminología consensuada. A su vez, los sistemas de HCE deben permitir la comunicación con otros colegas y con aplicaciones utilizadas por el paciente.

6. *Soporte al paciente:* La mayoría de las HCE proveen medios de salida para enviar información al paciente sobre condiciones de salud, estudios diagnósticos o tratamientos. Esta información mejora la relación médico-paciente y la educación de este último.

7. *Procesos administrativos:* Dependiendo del nivel de atención, la HCE puede estar íntimamente ligada a los procesos administrativos mediante la programación electrónica de visitas, el envío electrónico de cobro de prestaciones, la verificación de la elegibilidad, los mensajes automatizados de renovación de recetas de fármacos, el empadronamiento automático de pacientes para la investigación y la inteligencia artificial.

8. *Sistema de reportes y de salud pública:* Las nuevas HCE permiten el reporte a bases de datos nacionales de forma automática. Otros sistemas pueden permitir el enrolamiento de pacientes en ensayos clínicos, entregando al paciente información sobre cómo seguir un protocolo.

9. *Emisión de informes médicos, de alta y de consulta:* De la misma manera que debe brindar soporte para el manejo de órdenes médicas y de resultados, debe posibilitar las múltiples formas de visualizar la información y agregar datos para diferentes informes asistenciales (González y Luna 2012).

6.5 PROBLEMAS DE LA HISTORIA CLÍNICA EN PAPEL

La historia clínica convencional o en papel, plantea algunas dificultades, entre las que pueden citarse las siguientes:

— Desorden y falta de uniformidad de los documentos.

— Información ilegible.

— La información no es inalterable.

— Cuestión de disponibilidad, acceso a la información.

— Errores en el archivado parcial.

— Dudosa garantía de confidencialidad. Incluso con un control riguroso de accesos la historia circula por el centro sanitario.

— Deterioro del soporte documental debido a accidentes como el agua y el fuego.

— Dificultad de separar los datos de filiación de los clínicos (Carnicero Giménez *et al.,* 2003).

Estas dificultades son más fáciles de resolver en el caso de la historia clínica electrónica, cuya implantación no debe suponer una distor-

sión de la actividad clínica, la informatización de la historia además de facilitar la solución a los problemas anteriores, es una oportunidad para llevar a cabo la integración de información clínica, y para revisar la organización de los servicios y de los profesionales.

6.6 RECOGIDA Y PRESENTACIÓN DE LOS DATOS

Los datos pueden recogerse con intervención de una persona o pueden ser capturados directamente de la fuente, sin esa intervención:

— *Personal:* es el más utilizado en los sistemas de salud, se produce cuando la información es generada o modificada por una persona. Puede ser directo, cuando la persona que la produce la introduce en el sistema, e indirecto cuando se utiliza otra persona interpuesta. El registro de información con carácter personal puede seguir el modelo del lenguaje natural o el modelo estructurado.

— *No personal:* se produce cuando la información se captura directamente desde dispositivos y máquinas, volcándose directamente en el sistema. En la actualidad todos los dispositivos que generan datos binarios disponen de interfaces que permiten la captura directa, aunque pueden presentar problemas de captura (Carnicero Giménez *et al.,* 2003).

La recogida de datos es la integración de la información generada por diferentes aplicaciones, en distinto momento y lugar. Para la integración de toda esa información se hace necesario un identificador de la persona, que sea inequívoco y unívoco.

La presentación de los datos está condicionada por las necesidades y el contexto de los usuarios del sistema. Se suele utilizar la palabra informe cuando la presentación es en forma de papel y de vista cuando esa representación es en una pantalla o método de proyección. La historia clínica electrónica debe propiciar el uso de las vistas relegando los informes en papel a aquellas situaciones en las que no se tenga acceso al sistema por medios electrónicos o por imperativo de la norma (González y Luna, 2012).

6.7 CARACTERÍSTICAS DE LA HISTORIA CLÍNICA ELECTRÓNICA

La informatización de la historia clínica es una oportunidad para introducir cambios sustanciales en el concepto clásico de historia, es más que informatizar el clásico registro en papel. Carnicero Giménez (2004) señala algunas características que la definen y la diferencian del registro tradicional:

— *Completa:* de todos los episodios de un paciente, con independencia de cuando se hayan producido y donde haya sido atendido.

— *Interoperable:* con otros sistemas como los departamentales, es decir, que integre la información de otros sistemas, como los de los laboratorios, servicios de diagnóstico por imagen, o los clínico-administrativos entre otros. Incluso debería considerarse la integración de datos procedentes de instrumentos de medida que manejen los pacientes o sus propios ordenadores. Pero la historia no solo se relaciona con otras aplicaciones clínicas, sino con las clínico-administrativas, de gestión económico-financiera y de gestión del conocimiento.

— *Accesible:* la historia clínica debe ser accesible en cualquier momento y lugar en que sea necesaria para atender al paciente. Con las limitaciones debidas a la legislación de protección de datos, también debe poder ser utilizada por los investigadores y profesionales de salud pública entre otros. Los pacientes, también de acuerdo con las leyes vigentes, deben tener acceso a su historia.

— *Flexible:* que permita su utilización a los investigadores, planificadores y evaluadores de la calidad de los servicios entre otros. La historia debería tener una estructura que permitiera el acceso a esa información ocultando los datos de identificación cuando no sean imprescindibles, y además estar organizada de forma que los datos pudieran ser explotados con facilidad.

— *Segura y confidencial:* todos los accesos a la historia deben ser registrados y debe identificarse quién accede y qué información introduce o modifica; algunos autores incluso indican que el

paciente debe conocer quién ha accedido a qué[79]. Para garantizar la seguridad y la confidencialidad resultan imprescindibles los procesos de seguridad que se han explicado precedentemente: autentificación, autorización, disponibilidad, integridad y no repudio.

La historia clínica debe diseñarse teniendo en cuenta que su función principal es servir de instrumento de trabajo a los médicos y demás personal sanitario en la atención de los pacientes. Por lo tanto, la informatización de la historia deben hacerla personas que estén familiarizadas y conozcan las tareas clínicas, los datos que son relevantes, las posibles soluciones a los problemas que se presenten y cómo evaluar cada una de esas soluciones con los usuarios. Las historias clínicas deben diseñarse para ayudar a los médicos a encontrar información relevante que pueda ser interpretada con rapidez y sin errores.

Señalan González y Luna (2012) que, en muchas ocasiones el diseño de la historia clínica parece estar determinado más por razones históricas, normas arbitrarias y usos no clínicos, tales como procedimientos legales, que por la necesidad de dar soporte a la interpretación de los datos en la gestión clínica, estas cuestiones no se tienen en cuenta produciéndose fracasos en la implantación de los sistemas de historia clínica.

6.8 LA INFORMACIÓN INTEGRAL DE SALUD

La información de salud no es un sistema aislado, forma parte de un sistema que incluye las aplicaciones clínico-administrativas, la de planificación y gestión, y los sistemas de ayuda a las decisiones clíni-

---

[79] «b) Registro de accesos producidos a sus conjuntos de datos: el ciudadano puede realizar el seguimiento de los detalles de los accesos realizados desde este sistema a sus propios conjuntos de datos, a fin de poder verificar la legitimidad de los mismos. Dispondrá para ello de información relativa al momento en que se realizó el acceso, Servicio de Salud, centro sanitario y servicio desde el que se realizó cada acceso, así como las características del documento electrónico accedido. Instituto de Información sanitaria (2009): *«El Sistema de Historia Clínica Digital del SNS»* [en línea]: http://www.msssi.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf [Consulta: 28/03/2015]

cas, entre otros. Además de lo anterior, el sistema clínico incluye no solo el registro de la relación entre el paciente y el profesional que le atiende, sino que integra los sistemas departamentales y todos aquellos que contienen información sobre su salud, con independencia del centro sanitario en el que se haya originado (Falagán *et al.,* 2003).

La nueva historia clínica, por lo tanto, no se reduce solo a la información relativa a un paciente en un centro sanitario, sino a toda la información de salud de un ciudadano, con independencia de dónde y cuándo haya sido generada. La historia forma parte de un sistema de información clínica que integra todos los sistemas clínicos o clínicos-administrativos. Este sistema permite garantizar la continuidad de la asistencia al mejorar la comunicación entre clínicos y el acceso de estos a toda la información de salud de un paciente, también permite garantizar la continuidad de la atención con los programas de prevención, los programas de salud laboral y la gestión de las prestaciones que se generan en su proceso; pero además, ese sistema clínico debe formar parte del sistema de información del servicio de salud correspondiente.

El sistema clínico se relaciona directamente con la gestión económico-financiera, por ejemplo, a efectos de facturación y contabilidad de costes; una importante utilidad de un sistema integrado es la relación entre la información clínica y la planificación estratégica y el control de gestión. La consolidación de la información clínica con la económico financiera y de recursos humanos proporciona las bases para la planificación estratégica y el control de gestión (Carnicero, Rojas de la Escalera y Blanco, 2014).

6.9 REQUISITOS NECESARIOS PARA EL DISEÑO, DESARROLLO E IMPLANTACIÓN DE UNA HISTORIA CLÍNICA ELECTRÓNICA

6.9.1 LA IDENTIFICACIÓN UNÍVOCA DE INDIVIDUOS

Tanto a nivel local como nacional, la mayor dificultad para integrar la información clínica de una persona reside en el mecanismo de identificación unívoca de esta (Carnicero, 2003). El foco del problema ya no está en la obtención de un identificador universal, sino que

ha migrado a servicios de identificación que contemplen tanto el proceso de acreditación de identidad como la correlación de múltiples padrones de individuos y una permanente auditoría que asegure la calidad de los datos en el maestro único de pacientes.

El acceso a la información geográficamente distribuida requiere un identificador único, para conseguir toda la información del paciente a nivel nacional; es esencial, conseguir un método de identificación eficaz, que pueda identificar toda la información existente de un paciente en las distintas comunidades. Actualmente, en las Comunidades Autónomas de España, existen un número de registros médicos que pueden ser gestionados dentro de esa comunidad, por un identificador único, pero solamente por esa comunidad. El entorno sanitario completo, incluyendo los pacientes, los proveedores y los organismos reguladores, se beneficiarán de la elaboración y aplicación de un identificador único del paciente.

Un identificador único del paciente tiene el potencial suficiente para asegurar un rápido acceso a su información sanitaria, la entrega oportuna de la atención, la vinculación de los historiales médicos de toda la vida de las personas, la agregación de información de salud para el análisis y la investigación.

La identidad de un individuo se compone de un conjunto de caracteres personales por los que ese individuo puede ser reconocido.

— El Identificador del paciente es el valor asignado a una persona, para facilitar la identificación positiva de esa persona para fines de asistencia sanitaria.

— El Identificador único del paciente es el valor asignado permanentemente a una persona, para fines de identificación y es único en todo el sistema nacional de salud.

— El Identificador único del paciente no es compartido con ningún otro individuo.

El Identificador del paciente debe ser único para cumplir los objetivos de cuidados intensivos del paciente, que son necesarios para el acceso a la atención y la información del paciente. Si la identificación de un paciente no es única dentro del Sistema Nacional de Salud, se pueden presentar riesgos y desafíos importantes.

Un identificador de paciente único en todo el Sistema Nacional de Salud de España, facilitará:

— Las aplicaciones para la integración de toda la información de un mismo paciente.
— Reducir los costes de las entidades sanitarias y la complejidad.
— Disminuirán los posibles errores médicos en el tratamiento del paciente. Asegurará el acceso oportuno a la información de los pacientes, con fines administrativos y de investigación (González del Alba, 2015).

6.9.2 INTEGRACIÓN CON OTROS SISTEMAS O INTEROPERABILIDAD

Se define como interoperabilidad a la habilidad de dos o más sistemas (o componentes de estos) para intercambiar y usar la información que ha sido enviada. La HCE no debe ser entendida como una isla. Requiere información de otros sistemas (de la institución o fuera de ella), por lo que es necesario desarrollarla teniendo en cuenta la posibilidad de intercambio electrónico de datos entre ellos. Esto puede lograrse mediante la creación de interfaces dedicadas para cada caso, algo útil cuando son pocos los sistemas a interrelacionar pero difícil de lograr y muy costoso cuando aumenta la cantidad de sistemas a integrar. Existen diferentes niveles de interoperabilidad e idealmente se logra mediante el uso de estándares (González y Luna 2012).

Desde el punto de vista de la informática aplicada a la salud, el *Institute of Medicine of the National Academies* (IOM) usa la siguiente definición: «Interoperabilidad es la habilidad de los sistemas para trabajar juntos, en general gracias a la adopción de estándares. La interoperabilidad no es solamente la habilidad de intercambiar información sanitaria, sino que requiere la habilidad de entender lo que se ha intercambiado» (Institute of Medicine, 2004).

Uno de los requisitos fundamentales para la implantación de la e-Salud es la interoperabilidad entre sistemas, concebida como la capacidad de varios sistemas o componentes para intercambiar información, entender estos datos y utilizarlos. De este modo, la información es compartida y está accesible desde cualquier punto de la red asistencial en la que se requiera su consulta y se garantiza la coherencia y calidad de los datos en todo el sistema, con el consiguiente beneficio para la continuidad asistencial y la seguridad del paciente. La pieza

fundamental de la interoperabilidad de sistemas es la utilización de «estándares» que definan los métodos para llevar a cabo estos intercambios de información.

Para Selene Indarte (2012: 317-329) los diferentes tipos de interoperabilidad son los siguientes:

— *Sintáctica:* centrada en la definición de la sintaxis para la construcción de los mensajes que los sistemas de información emplean para intercambiar datos.

— *Semántica:* para la interpretación homogénea de los datos intercambiados transmitidos o recibidos. De este modo, cada sistema puede incorporar la información recibida a sus propias bases de datos sin necesidad de realizar ningún análisis ni procesamiento.

— *Organizativa:* basada en la definición de reglas de negocio y procedimientos de actuación que regulen la participación de los distintos actores en los procesos de la organización.

Para el desarrollo de la interoperabilidad es fundamental tener en cuenta los siguientes requisitos:

— Adaptación de sistemas de información y adopción de estándares en tres niveles: sistemas, red e infraestructura de información y servicios (interconexión de redes).

— Utilización de estándares tecnológicos (HL7, DICOM, CDA y otros) y semánticos (CIAP2, CIE9, CIE10, SNOMED CT, entre otros).

6.9.3 ESTÁNDARES

La necesidad de estándares en sus diferentes aspectos es un tema que lleva muchos años y es una de las barreras más reconocidas para la difusión y adopción de las HCE (González y Luna, 2012). En el desarrollo e implementación de las HCE existe una gran cantidad de estándares a utilizar, entre los que se puede citar aquellos orientados al intercambio de datos y mensajería electrónica, de terminología, de documentos, conceptuales, de aplicación y por último de arquitectura (Kim, 2005).

De acuerdo con la Organización de Estandarización Internacional, un estándar o norma es un documento establecido por consenso y aprobado por un organismo reconocido, que provee, para un uso repetido y rutinario, reglas, guías o características para las actividades o sus resultados, dirigidas a la consecución de un grado óptimo de orden en un contexto dado. Las normas pueden ser oficiales o «de facto». Una norma oficial es un documento público, elaborado por consenso, de acuerdo con un procedimiento establecido con el respaldo de un organismo reconocido.

En general, un sistema de HCE es una estructura compleja. Los sistemas o servicios de HCE incorporan muchos elementos de información. En consecuencia, existen diferentes conjuntos de normas que se aplican a los diferentes componentes del sistema.

Entre estos cabe destacar:

— Estándares de contenidos y estructura (arquitectura).

— Representación de datos clínicos (codificación).

— Estándares de comunicación (formatos de mensajes).

— Seguridad de datos, confidencialidad y autentificación.

En la actualidad existen seis aproximaciones principales que están compitiendo por ser la plataforma para la interoperabilidad en HCE:

— OSI (*Open Systems Interconnection*).

— CORBA (*Common Object Request Broker Architecture*).

— GEHR (*Good European Health Record*).

— HL7-CDA (*Clinical Document Architecture*).

— openEHR y la aproximación genérica XML/Ontología.

En la clasificación tradicional de normas se distingue entre:

a) *Normas nacionales:* son elaboradas, sometidas a un período de información pública y sancionadas por un organismo reconocido legalmente para desarrollar actividades de normalización en un ámbito nacional. En España estas normas son las normas UNE (Una Norma Española), aprobadas por AENOR, que es el organismo reconocido por la Administración Pública española para desarrollar las actividades de normalización oficial en nuestro país.

b) *Normas regionales:* son elaboradas en el marco de un organismo de normalización de una región del mundo, normalmente de ámbito continental, que agrupa a un determinado número de organismos nacionales de normalización. Las más conocidas, aunque no las únicas, son las normas europeas elaboradas por los Organismos Europeos de Normalización (CEN, CENELEC, ETSI), y preparadas con la participación de representantes acreditados de todos los países miembros.

c) *Normas internacionales:* tienen características similares a las normas regionales en cuanto a su elaboración, pero se distinguen de ellas en que su ámbito es mundial. Las más representativas por su campo de actividad son las normas ISO, elaboradas por la Organización Internacional de Normalización ISO *(International Standards Organiza*tion). AENOR es el organismo nacional de normalización español miembro de ISO.

International Organization for Standardization (ISO) es la organización de alcance mundial en la que opera el Comité ISO TC215. En Europa la autoridad es CEN (Comité Europeo de Normalización) en el que participan los organismos nacionales como es el caso de AENOR en España e IBNORCA en Bolivia. ANSI *(American National Standards Institute)* es el organismo oficial de Estados Unidos que coordina las actividades nacionales de normalización en informática, para la salud mediante el HISPP *(Healthcare Informatics Standards Planning Panel)*. Este comité canaliza la participación de los grupos de normalización de varias organizaciones independientes como son HL7, DICOM, ASTM, IEEE y SNOMED.

6.9.4 LA ADECUADA REPRESENTACIÓN DE LA INFORMACIÓN CLÍNICA

Se debe tener en cuenta que los miembros del equipo de salud están habituados a registrar su actividad asistencial mediante texto narrativo. Esta forma de registro mantiene gran cantidad de información contextual necesaria para la comunicación con sus pares y asegurar un correcto proceso diagnóstico y terapéutico. Sin embargo, la información descripta en texto narrativo puede ser ambigua, ya que varios conceptos pueden estar representados por un mismo término (polisemia) o un mismo concepto representado por varios términos (sinonimia). Lo antedicho suele representar un problema im-

portante para las computadoras. La codificación (acción de ponerle un código a algo) de ese texto narrativo se presenta como una de las soluciones. Otra solución para disminuir la ambigüedad es obligar el ingreso estructurado de información, lo que permite su rápida utilización por los sistemas de información necesarios para alimentar los sistemas de soporte para la toma de decisiones y para el análisis posterior de datos agregados. Sin embargo, la codificación primaria y el ingreso estructurado no son siempre bien recibidos por los profesionales (González y Luna, 2012).

6.9.5 ASPECTOS RELACIONADOS CON LA USABILIDAD

Los tópicos referidos con la usabilidad y el diseño de las interacciones humano-computadora correlacionan directamente con la aceptación y uso de la HCE por parte de sus usuarios. Una ergonomía adecuada de los aplicativos es uno de los aspectos más importantes a tener en cuenta para dar soporte a un proceso de documentación clínica efectivo, eficiente y facilitador del trabajo cotidiano (González y Luna, 2012).

6.9.6 ASPECTOS LEGALES

Debido a que las tecnologías relacionadas con las HCE son relativamente nuevas en los diferentes países en donde se implementan, todavía se están discutiendo y debatiendo muchos aspectos legales. Sin embargo, existen varios países en los cuales esta problemática ya está resuelta, por ejemplo en España y Bolivia, donde el soporte electrónico tiene la misma validez legal que el tradicional en papel (Carnicero, 2003). El reconocimiento del valor probatorio de los documentos electrónicos es un requisito indispensable para la implementación de la HCE (González y Luna, 2012).

6.9.7 SEGURIDAD, PRIVACIDAD Y CONFIDENCIALIDAD

Los aspectos relacionados con la privacidad de los datos de los pacientes constituyen un aspecto muy importante a tener en cuenta. Los profesionales dudan de la seguridad de la HCE para almacenar la

información y plantean reparos ante la posibilidad de accesos no autorizados, preocupándose del tema aún más que los mismos pacientes (Simon, 2007). Incluso entre los médicos que usan una HCE, la mayoría cree que existen mayores riesgos atinentes a la seguridad y confidencialidad en el formato electrónico que en la historia clínica en papel. Sin embargo, cabe señalar que hasta las implementaciones más básicas de HCE son más seguras que los actuales archivos físicos de registros en papel, así como la implementación de perfiles de acceso que aseguran limitaciones al acceso de la información contenida en la HCE. Es necesario tomar las medidas necesarias para asegurar una adecuada división de entornos de desarrollo, testeo y producción de sistemas, otorgamiento de perfiles de usuario y accesos, así como el registro sistemático del quehacer de los usuarios en el sistema que posibilita su trazabilidad, algo imposible de lograr en los tradicionales registros en papel (González y Luna, 2012).

6.9.8 MANEJO DEL CAMBIO

Este es uno de los aspectos más relevantes a tener en cuenta para la implementación de la HCE. La resistencia al cambio que presentan los miembros del equipo de salud es una constante en todos los procesos de informatización del registro clínico en las instituciones. Entender estas implementaciones desde un punto de vista socio-técnico ayudará a considerar el compromiso de los referentes de todas las áreas involucradas en el proceso asistencial. La creación de un equipo multidisciplinario para la definición de los alcances y la planificación de las tareas relacionadas con el diseño o eventual selección de una HCE es un factor primordial para lograr una implementación exitosa (Souther, 2001).

6.9.9 MANEJO DE LA TRANSICIÓN

Debe tenerse en cuenta la problemática asociada al período comprendido desde que se deja la historia clínica en papel y se comienza a usar la electrónica. Las inconsistencias entre la información contenida en los registros médicos en papel y los electrónicos pueden llevar a problemas significativos para los miembros del equipo de salud en su práctica diaria. Además, debería evitarse la denominada paradoja

del papel, en donde luego de la informatización no se logra reducir el uso de papel en la organización sino que, por el contrario, a veces aumenta (Stausberg y otros, 2003).

6.9.10 PÉRDIDA DE PRODUCTIVIDAD

Al menos al inicio de las implementaciones es de esperar una sensación de pérdida de productividad por parte de los profesionales. Las HCE impactan en el tiempo de documentación. De la misma manera, con solo brindar acceso a información clínica centralizada de los diferentes niveles de atención (sin sistemas de soporte para la toma de decisiones) ya se mejora la toma de decisiones durante el proceso asistencial. Esto es algo que, alcanzada la meseta de acostumbramiento de los cambios (alrededor de 6 meses), los médicos perciben claramente (Poissant y otros, 2005).

6.10 USUARIOS DE LA INFORMACIÓN DE SALUD

Los posibles usuarios de la información de salud son los profesionales que le atiendan a un paciente en un centro de salud, en su domicilio, en un consultorio rural aislado, en la ambulancia medicalizada, en la consulta externa de un hospital o cuando está ingresado, pero, también puede precisar el acceso a esa información en España el personal de emergencias que atiende el teléfono 112, médicos y enfermeras en este caso; aquellos que atienden un centro de contactos para teleasistencia; las oficinas de farmacia y los servicios de salud laboral. También deben poder acceder a su propia historia los pacientes o ciudadanos (Mazón y Carnicero, 2001).

Todos ellos no tienen que poder acceder a toda ni a la misma información, deben establecerse los perfiles de usuario, que permitan el acceso a unas vistas que serán diferentes según el perfil de la persona que accede. Estos aspectos están directamente relacionados con la gestión de la seguridad y confidencialidad de la información clínica (González y Luna, 2012).

Es frecuente que sea necesario permitir accesos a la historia clínica de un paciente desde diversos departamentos de un mismo centro y por distintos profesionales, con distintas necesidades, por ello el siste-

ma informático deberá atribuir perfiles[80] (médico, especialista, fisioterapeuta, enfermera de planta, técnico de laboratorio, administrativa, etc.) y diseñar la historia de forma que las personas puedan acceder a los apartados que sean necesarios para la función asistencial que desempeñan y se impida el acceso a aquellas partes de la historia clínica respecto de las que no estén legitimados (Martí y Pidevall, 2004).

6.11 LA SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN CLÍNICA

Tradicionalmente la seguridad de los accesos en la historia clínica en soporte papel ha venido dada por el control físico del acceso a la documentación (armario cerrado con llave en posesión exclusivamente del personal autorizado o de gestión del archivo por personal encargado del mismo el cual verificará la legitimación para acceder) y por la garantía de autoría y de integridad del contenido de la historia al ser ésta escrita del puño y letra del profesional responsable y quedar constancia de cualquier modificación (Martí y Pidevall, 2004).

La accesibilidad a la información clínica en cualquier tiempo y lugar es uno de los principales beneficios de la historia clínica electrónica integrada en el sistema de información de salud, pero todos esos beneficios pueden anularse si no se garantiza su seguridad y confidencialidad. Entre los médicos existe la inquietud de si esa garantía existe o no, lo que puede formar parte de las barreras culturales para la implementación de la historia clínica electrónica (Carnicero *et al.*, 2002).

La informatización de la historia clínica ha hecho necesario adoptar nuevas medidas de seguridad para el control de accesos y del uso

---

80 Interoperabilidad Técnica. Política de estándares para el SNS: «… La comunicación entre las diferentes CCAA y el Ministerio de Sanidad se realiza a través de la Intranet Sanitaria, red privada de comunicación que habilita el acceso a estos servicios únicamente a los agentes autorizados para las transacciones, y permite garantizar los niveles de seguridad, disponibilidad y calidad de servicio, que estos servicios requieren por su criticidad». Instituto de Información sanitaria (2009): *«El Sistema de Historia Clínica Digital del SNS»* [en línea]: http://www.msssi.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf [Consulta: 28/03/2015].

de la información que se encuentra en los ordenadores, tratando de preservar así la intimidad de los pacientes.

La historia clínica electrónica no es menos segura ni garantiza menos la confidencialidad que la historia en papel, existen procedimientos para garantizar esa seguridad y confidencialidad, que por otro lado exigen tanto la normativa sanitaria como la de protección de datos. Esos procedimientos son los que permiten garantizar la identidad de la persona que accede, la autorización con que cuenta, la disponibilidad de la información, la integridad de esta y el no repudio a las anotaciones o consultas llevadas a cabo en la historia (Sanz y Hualde, 2001).

La exigencia de la garantía de confidencialidad de la historia clínica ha comportado que los centros asistenciales adopten medidas para la delimitación de las personas que pueden acceder a cada una de las historias clínicas, creando una lista de accesos y asignando un responsable de los cambios que se hagan en la lista, se trataría de la figura del administrador de accesos a las historias clínicas (Martí y Pidevall, 2004).

— *Identificación del usuario:* los técnicos suelen utilizar el término autenticación o autentificación. Existen técnicas que lo permiten con seguridad, como mecanismos biométricos, contraseñas, tarjetas chip y certificados digitales entre otros.

— *Autorización:* determinar a qué información puede acceder y qué tareas puede acometer, una persona autentificada, por lo tanto identificada con certeza, este proceso determina los privilegios asociados a un perfil de usuario, en función de ese perfil se determina las vistas de la información; el perfil del usuario se define según su función y necesidad (médico, especialista, fisioterapeuta, enfermera de planta, técnico de laboratorio, administrativa, etc.) Estos sistemas se basarían en comprobar que el solicitante de acceso está familiarizado con el paciente y su condición antes de que le sean presentados los datos (Blanco y Rojas, 2012).

— *Disponibilidad:* forma parte de la seguridad poder disponer de la información cuando se necesite, para ello se deben proteger los sistemas con el fin de mantenerlos en funcionamiento, de forma que se pueda acceder a la información en cualquier momento. Con la historia clínica en papel se plantean problemas de disponibilidad, entre otros cuando el paciente es atendido en un centro distinto del habitual, cuando la historia no se localiza o cuando el archivo está cerrado. Con la historia clínica

electrónica el problema se puede plantear cuando el sistema falla, o se destruye o modifica indebidamente la información, para prevenir estos hechos se debe contar con un plan de seguridad (Pérez Campanero, 2001).

— *Confidencialidad:* para asegurar que a la información solo accede quien está autorizado para ello, para garantizarlo se utilizan mecanismos de encriptación o cifrado.

— *Integridad:* es el conjunto de acciones dirigidas a garantizar que la información no se ha transformado durante su proceso, transporte o almacenamiento. Se utiliza la firma electrónica.

— *No repudio:* procedimientos para asegurar que ninguno de los profesionales implicados, ya identificados (autentificados), pueda negar haber participado en una determinada transacción, se utilizan mecanismos de encriptación y firma electrónica.

Es importante indicar que la gestión de la seguridad y de la confidencialidad no es un asunto de los informáticos ni son problemas técnicos. Señala Carnicero Giménez (2004:288) que «la gestión de la seguridad y confidencialidad requiere un compromiso de la alta dirección, pero también de todos y cada uno de los implicados en el proceso asistencial y en el tratamiento de la información».

Por otra parte, la gestión de seguridad y confidencialidad requiere organización y que estén definidas cuestiones como quién puede acceder a la información y a qué información (que los perfiles y las vistas estén definidos) y quién y cómo concede las autorizaciones, todo ello debe formar parte del plan de seguridad de la información que veremos en extenso más adelante (Martínez y Rojas, 2014).

6.12 DIRECTRICES PARA DISPONER DE UN SISTEMA SEGURO

Durante el diseño de una solución deben identificarse las áreas vulnerables en las que alguien, de forma intencionada o involuntaria, pueda comprometer la seguridad del sistema. Para proteger los elementos de un sistema de información deben seguirse las siguientes directrices:

— *Infraestructuras de comunicaciones:* en el caso de cables, *routers*, cortafuegos *(firewalls)* y *switches*, se asegurará la integri-

dad del tráfico que transporta la red, protegiéndolo frente a las amenazas que pudieran detectarse, como son los ataques basados en TCP/IP y *passwords*.

— *Máquinas:* en los servidores Web, de datos, y de aplicaciones, se deberían tener en cuenta aspectos como parches y actualizaciones, servicios, protocolos, cuentas de usuario, puertos de comunicaciones, ficheros y carpetas, entre otros.

— *Programas y datos:* se deben tener en cuenta aspectos como validación de las entradas de datos por parte de los usuarios, gestión de perfiles de acceso, autorización con que cuentan estos perfiles, configuración de las conexiones, encriptación, gestión de errores y auditoría (Carnicero Giménez *et al.,* 2003).

Se debe alcanzar un equilibrio entre seguridad y disponibilidad. Un exceso de medidas para garantizar la confidencialidad puede colapsar los sistemas y comprometer el acceso a la información, de forma que se impida cumplir la principal función de la historia clínica informatizada, que es la asistencial. Por otra parte, la falta de medidas suficientes de seguridad, puede comprometer la confidencialidad y generar desconfianza entre los clínicos, de forma que se dificulte la implantación y se impida el aprovechamiento de todas las ventajas que suponen la utilización de las TIC para la calidad y eficiencia de la atención sanitaria (Carnicero, Rojas de la Escalera y Blanco, 2014).

La seguridad, confidencialidad y disponibilidad de la información clínica requieren medidas de organización, la primera de las cuales es conseguir que todos los implicados en el problema lo conozcan y sean sensibles a la importancia que tiene para las personas que atienden.

6.13 ESTÁNDARES PARA LA HISTORIA CLÍNICA ELECTRÓNICA

La gestión integrada de los servicios sanitarios y la continuidad de los cuidados requiere la adopción de mensajes, formatos, codificación y estructura de las historias clínicas, de tal forma que permitan la interoperabilidad de los sistemas de información sanitaria.

Un estándar o norma es un documento establecido por consenso y aprobado por un organismo reconocido, que provee, para un uso repetido y habitual, reglas, guías o características para las actividades o

sus resultados, dirigidas a la consecución de un grado óptimo de orden en un contexto dado.

Existen diferentes conjuntos de normas que se aplican a los diferentes componentes del sistema de historia clínica informatizada, entre los que se destacan:

— Estándares de contenido y estructuras (arquitectura).

— Representación de datos clínicos (codificación).

— Estándares de comunicación (formatos de mensajes).

— Seguridad de datos, confidencialidad y autentificación.

En la clasificación de normas se distingue entre las nacionales (UNE), regionales (CEN, CENELEC y ETSI) e internacionales (ISO).

El Comité Europeo de Normalización (CEN) en este momento está proponiendo un nuevo estándar prENV 13606-1. Esta norma específica la arquitectura de información requerida para las comunicaciones interoperables entre sistemas y servicios que proveen o necesitan datos de la historia clínica electrónica.

Este nuevo estándar revisado consta de cinco (5) partes:

— *Parte 1 Modelo de Referencia:* un modelo de información genérico para comunicar con la historia clínica electrónica de cualquier paciente, que es un refinamiento de la Parte 1 de ENV 13606.

— *Parte 2 Especificación de intercambio de arquetipos:* un modelo de información genérico y un lenguaje para la representar y comunicar la definición de instancias individuales de arquetipos.

— *Parte 3 Arquetipos de referencia y listas de términos:* un rango de arquetipos reflejando una diversidad de requisitos clínicos y condiciones, como un «conjunto de arranque» para los adoptadores y para ilustrar cómo otros dominios clínicos podrían representarse de forma similar (por ejemplo por grupos de profesionales sanitarios), y más listas (normativas o informativas) para soporte de otras partes de este estándar. Esto se correlacionará con ENV 13606.

— *Parte 4 Características de seguridad:* define los conceptos del modelo de información que se necesitan reflejar dentro de instancias de HCE individuales para permitir una interacción apropiada con los componentes de seguridad que pudieran ser

requeridos en cualquier implantación futura de HCE. Se construye sobre la ENV 13606 Parte 3.

— *Parte 5 Modelos de Intercambio:* contiene un conjunto de modelos que se construyen sobre las partes anteriores de la norma y pueden formar el soporte de comunicaciones basadas en mensajes o en servicios, cumpliendo el mismo papel que la ENV 13606 (González del Alba, 2015).

En el desarrollo del nuevo estándar se ha mantenido una estrecha colaboración entre representantes de CEN, openEHR y HL7 a fin de armonizarlo tanto con el modelo de información y enfoque por arquetipos de openEHR así como con la Arquitectura de Documentos Clínicos y Plantillas de HL7.

Health Level 7 (HL7) es una organización con base en Estados Unidos dedicada al desarrollo de estándares en el campo de la información sanitaria, que está acreditada por la autoridad oficial de estandarización americana. Está enfocada al desarrollo de especificaciones de mensajería en el «nivel de aplicación», nivel 7 del modelo OSI, entre sistemas de información sanitaria, documentos clínicos y soporte a la decisión.

El eje funcional es una jerarquía de las funciones esenciales, deseables y opcionales de HCE a lo largo de todos los sitios de cuidados, con funciones organizados en sitio de asistencia y categorías de infraestructuras. Cada lugar de asistencia, por ejemplo, consultas externas, ambulatorios, etc. tienen un perfil normativo que lo acompañan para definir cómo se usan las funciones definidas e identificando cualquier función específica del sitio de asistencia.

El EHR SIG está coordinando la definición de los lugares de asistencia con el *Institute of Medicine* (IOM), que está comprometido en la publicación de un informe sobre seguridad de los pacientes. En la actualidad existe un alto grado de colaboración entre CEN y HL7 para la definición de CMET y GPIC, que sirven para propósitos generales, y sobre un conjunto armonizado de tipos de datos (González del Alba, 2015).

ISO *(International Organization for Standarization)* es una federación mundial de organismos nacionales de normalización que son miembros de ISO. El trabajo de preparación de las Normas Internacionales se realiza a través de Comités Técnicos ISO. La publicación como un Estándar Internacional requiere la aprobación por al menos el 75%

de los organismos miembros. ISO es conocida por su amplia gama de estándares utilizados en numerosos aspectos de sistemas de información, que tienen lugar dentro del *Joint Technical Committee* (JTC).

La Especificación Técnica ISO 18308 requisitos de la arquitectura de la historia clínica electrónica *(Requirements for an Electronic Health Record Reference Architecture)* contiene un conjunto de requisitos clínicos y técnicos para una arquitectura de historia clínica que soporta el uso, compartimiento e intercambio de registros electrónicos a través de diferentes sectores de salud, diferentes países y diferentes modelos de asistencia sanitaria.

El desarrollo de la ISO 18308 se ha producido en tres (3) etapas:

— En la primera se realizó una búsqueda exhaustiva de material de referencia a través de la literatura y contactos directos seleccionándose 35 fuentes primarias incluyendo 20 fuentes originalmente recogidas por el proyecto EHCR-SupA en Europa.

— En la segunda fase se trabajó con los más de 700 requisitos identificados en la primera fase y se desarrolló una estructura jerárquica de «encabezamientos» bajo los cuales se podían organizar los requisitos. Tras eliminar las redundancias se quedaron reducidas al final de esta fase a 590.

— En la fase final se consolidó un conjunto de 123 requisitos listados bajo una estructura de 10 títulos y 60 subtítulos.

Otros tipos de estándares relacionados con la historia clínica electrónica están entre nomenclaturas SNOMED[81] y *Read Codes*[82]; clasi-

---

[81] SNOMED (*Systematized Nomenclature of Human and Veterinary Medicine*) es una estructura de codificación mantenida por el Colegio Americano de Patólogos (CAP) y está ampliamente aceptada para describir los resultados de pruebas clínicas. Tiene una estructura de codificación multiaxial con once campos lo que le confiere una mayor especificidad que otros tipos de codificación dándole un considerable valor para fines clínicos. SNOMED está coordinando su desarrollo actualmente con otras organizaciones de estandarización como HL7 y ACR-NEMA (DICOM). SNOMED es un candidato firme para convertirse en la nomenclatura estándar para sistemas de HCE.

[82] El READ *Classification System* (RCS), desarrollado por J. Read en los 80, es una nomenclatura médica multi-axial usada en el Reino Unido. Los READ *Clinical Codes* fueron adoptados por el *National Health Service* en 1990 y

ficaciones como, la Clasificación Internacional de la OMS y la Clasificación Internacional de Problemas de Salud WONCA, tesauros o lenguajes controlados como el *Medical Subject Headings* MeSH de la *National Library of Medicine*, y glosarios y agrupadores, como los grupos relacionados con el diagnóstico.

El estándar para la comunicación de imágenes diagnósticas médicas el estándar DICOM *(Digital Imaging and Communications)* ha sido desarrollado por el Colegio Americano de radiología y la NEMA *(National Electrical Manufacturer's Association)*. DICOM define los estándares de comunicaciones y formatos de mensajes para imágenes diagnósticas y terapéuticas.

DICOM está soportado por la mayoría de fabricantes de equipamiento radiológico y de PACS (*Picture Archiving and Communications Systems*). Este estándar se ha incorporado en la norma europea MEDICOM (*Medical Image Communication*). El estándar actual DICOM versión 3.0 recoge un gran número de mejoras en relación con las versiones anteriores que sólo eran aplicables para sistemas de comunicación punto a punto.

El estándar se ha desarrollado originalmente con el foco en imágenes diagnósticas tal como se práctica en Departamentos de Radiología y disciplinas asociadas, pero se puede utilizar también para el intercambio de imágenes en otros entornos clínicos. El estándar se ha construido siguiendo las normas ISO para multidocumento. Esto facilita la evolución del estándar en un entorno rápidamente cambiante. El estándar DICOM está diseñado para el intercambio de información digital entre equipos de imágenes médicas. No obstante este tipo de equipos pueden interoperar con otros dispositivos médicos, por lo que el alcance del estándar se solapa con otras áreas de informática médica (Rojas, Martínez y Elicegui, 2012).

6.14 IMPLANTACIÓN DE SISTEMAS DE INFORMACIÓN

La implantación de cualquier sistema de información requiere un proceso de análisis, especificación, adquisición, instalación, pruebas, mantenimiento y actualización. Estas fases se pueden aplicar al pro-

---

se han integrado en los sistemas de HCE. En este momento se han unido con SNOMED.

ceso de implantación de un sistema de historia clínica electrónica, pero conviene tomar en consideración las características específicas del sector sanitario y lo que realmente representa el concepto de historia clínica electrónica única que la experiencia va enseñando.

Así pues, convendría tener especialmente en cuenta los siguientes puntos que señala Martínez del Cerro (2004:530) que son muy específicos de estos sistemas:

— La estrategia para implantar un sistema de historia clínica tiene que ver más con la gestión de la información que con la informática.

— Es necesario adaptar los procedimientos de trabajo para buscar la eficiencia.

— Es esencial proporcionar una formación idónea a los usuarios y profesionales.

— Es más eficiente implantar los sistemas de manera gradual, evitando una implantación a gran escala al principio.

— Es más complejo mantener el sistema en funcionamiento que instalarlo.

— Es preciso definir distintos perfiles de usuario.

— Hay que implicar a todos los actores: compradores, proveedores, usuarios, operadores, etc., buscando apoyo en la experiencia.

No hay que esperar a tener tecnologías de la información y de las comunicaciones estables, sólidas y aceptadas por todas las partes.

6.15 VENTAJAS DE LA INFORMATIZACIÓN DE LA HISTORIA CLÍNICA

La historia clínica ha sido siempre una entidad dispersa. Definida literalmente es la acumulación de la información médica concerniente a un paciente, en condiciones ideales esta información se encuentra en una única carpeta con los datos de identificación en la cubierta. En la vida real esta diseminada entre varios archivos informatizados y en papel, en varias localizaciones y a menudo bajo varios números de identificación. Además, mucha de la información de las historias es

obsoleta, redundante, duplicada o indescifrable, hasta el extremo de que no beneficia al paciente en el punto de atención (Pérez Campanero, 2001).

La informatización de la historia clínica es una oportunidad para solventar estos inconvenientes y otros, como los referidos a la seguridad y confidencialidad. Las potenciales ventajas de la historia informatizada en relación con la historia convencional en papel pueden sintetizarse en los siguientes:

— *Acceso simultáneo y remoto:* la historia informatizada permite el acceso simultáneo de más de una persona a la información clínica y desde cualquier lugar, tiene la ventaja de que se accede a una información legible y de que no requiere sobres voluminosos ni grandes archivos que ocupan espacio en los centros sanitarios o se ubican en almacenes alejados de estos centros, con el problema de que entonces no siempre están accesibles cuando se precisan.

— El acceso remoto a la información clínica supone un potente instrumento para la integración de la atención primaria con la especializada, el compartir información clínica, entre la que se encuentran los resultados de las pruebas complementarias, es una forma muy eficaz de mejorar la comunicación entre niveles y puede considerarse imprescindible para garantizar la continuidad de la asistencia. La mejora de comunicación entre clínicos permite disminuir la posibilidad de cometer errores en la atención sanitaria; la integración de la información clínica permite la emisión de alertas y reduce los errores de transcripción al utilizar bases de datos comunes; facilita el acceso a las guías de práctica clínica; la utilización de sistemas de soporte a la decisión; la monitorización de los pacientes; y el control y seguimiento de eventos adversos (Carnicero Giménez, 2004).

— *Seguridad y confidencialidad:* cuando de tratan los aspectos de seguridad y confidencialidad de la historia se suele pensar siempre en estos últimos, sin embargo, una parte importante de la seguridad es la disponibilidad de la información cuando se la necesita. Además, de ello debe garantizarse la integridad de esa información y que solo tenga acceso quien está autorizado para ello y a la parte de información a que está autorizado, que es la que necesita por su función. La historia clínica electrónica per-

mite hacer frente a estas cuestiones de una forma más eficaz que la historia en papel (Pérez Campanero, 2001).

— *Procesado de la información:* la historia informatizada incorpora datos de varias fuentes de información, la directamente recogida por los profesionales sanitarios, la de los sistemas departamentales, que incluyen la información suministrada por equipos de diagnóstico, y la de los sistemas clínico-administrativos. Esta información es más fácil de procesar con sistemas informáticos, pero además este procesado se actualiza de forma permanente y se puede presentar e imprimir de acuerdo con las necesidades de cada momento.

— *Múltiples visualizaciones de los datos:* Las HCE también tienen el potencial de ofrecer múltiples visualizaciones de la información, ya que los usuarios pueden preferir ver un mismo dato en diferentes formatos de acuerdo con su necesidad. Una buena HCE debe permitir configurar las visualizaciones de los datos de distintas maneras y ofrecer estas opciones a los usuarios. Otra funcionalidad útil en la práctica clínica es la visualización de tendencias. Estas pueden generarse instantáneamente al graficarse tendencias de un valor de laboratorio o un signo vital (González y Luna, 2012).

— *Comunicación con otros profesionales:* La HCE puede funcionar como un vehículo para que los profesionales se comuniquen entre sí; y no solo entre los médicos sino también entre otros miembros del equipo de salud. Muchos sistemas de HCE incluyen aplicaciones similares al correo electrónico o la mensajería instantánea, de modo que diferentes profesionales pueden mandar mensajes a otros profesionales vinculados con la atención de ese paciente (González y Luna, 2012).

— *Comunicación con los pacientes:* Las HCE también pueden mejorar la comunicación con los pacientes. Como ya fue mencionado, la historia clínica personal de salud posee la potencialidad de generar un canal de comunicación entre el paciente y el equipo de salud que lo asiste (Tang y otros, 2006).

— *Agregación de datos:* La HCE también tiene la funcionalidad de recopilar datos, permitiendo crear resúmenes y agrupaciones con ellos. Obviamente para una agregación eficaz se requiere un minucioso control de calidad sobre el dato y una co-

rrecta representación del conocimiento médico (control semántico). Su aplicación permite la reutilización de la información almacenada para hacer gestión clínica, investigación clínica o para realizar reportes de salud pública, entre otros ejemplos (González y Luna, 2012).

— *Acceso a bases de conocimiento:* Otro beneficio potencial de las HCE es el acceso a bases de conocimiento de una manera contextual. Esto significa que la HCE puede proporcionar el contexto con respecto a la información de los pacientes y dar información útil al usuario para la toma de decisiones desde diferentes bases de conocimiento (Cimino y Del Friol, 2007).

— *Integración con el soporte para la toma de decisiones:* Estos sistemas computarizados de soporte para la toma de decisiones clínicas son difíciles de lograr y están poco desarrollados debido a la gran complejidad inherente a su creación e implementación. Están compuestos por un motor de reglas que utiliza información basada en el paciente (originada en la HCE) e información basada en el conocimiento científico (bases de conocimiento), con lo cual generan diferentes productos de salida tales como recordatorios, alarmas, sugerencias diagnósticas o terapéuticas por medio de la informatización de guías de práctica clínica y otros. Estos sistemas tienen el fin último de prevenir errores y mejorar la calidad asistencial. Una revisión de la literatura sobre este tipo de herramientas mostró evidencias claras sobre su beneficio en la conducta de los profesionales y una incipiente evidencia sobre mejoras clínicas en los pacientes (Chaudhry y otros, 2006).

— *Costo-beneficio:* Este es un tema claramente controversial y existe literatura que aporta evidencia a favor y en contra. En buena parte, esta discusión se debe a las diferentes perspectivas desde donde se analizan los retornos de la inversión o ROI (el médico individual, las instituciones prestadoras de servicios, las aseguradoras, los gobiernos) y el tipo de sistema sanitario predominante en cada país. Aún falta información pertinente para hacer un cálculo más adecuado del ROI de las HCE; sin embargo, una reciente revisión sistemática denota un beneficio económico en la implementación de HCE al menos a nivel organizacional, no regional o nacional (González y Luna, 2012).

— *Mejoras en la calidad de atención:* Un estudio reciente sobre la evidencia aportada por revisiones sistemáticas acerca del impacto de los sistemas de información en el ámbito de la salud muestra una mejora en la calidad de cuidado brindado con este tipo de sistemas. Asimismo, existen estudios que informan mejoras en la eficiencia de los profesionales y un aumento en la adherencia a guías de práctica clínica asociadas a la HCE (Furukawa, 2011).

Las historias clínicas electrónicas simplifican el quehacer diario del personal sanitario evitando la repetición de datos y la emisión de documentos como las recetas, informes, partes de baja y toda la documentación administrativa y legal relacionada con la atención sanitaria. Los sistemas informáticos admiten además que esa información fluya hacia otros sistemas como alarmas, farmacias y correo electrónico entre otros (González y Luna, 2012).

En resumen, las ventajas de la informatización de la historia clínica se refieren a la disponibilidad, el acceso, el procesado y la integración de la información, la seguridad y confidencialidad, y la prevención de errores.

6.16 DIFICULTADES Y DESVENTAJAS DE LA HISTORIA CLÍNICA INFORMATIZADA

La implantación de sistemas informáticos de historia clínica debe superar al menos dos tipos de dificultades: las financieras y las culturales. A estas dificultades se añaden la ausencia de estándares universalmente aceptados de transferencia de información y la mayor flexibilidad de la historia tradicional.

— *Dificultades financieras:* la incorporación de las TIC a la práctica clínica ha sido relativamente reciente, hasta ahora la investigación y desarrollo de sistemas informáticos en el área de la salud se habían dirigido a los programas de soporte a la gestión. Esta situación dificulta, encarece y retrasa la informatización de la actividad clínica porque no existen soluciones universalmente aceptadas. Se produce además la circunstancia de que es muy frecuente el que firmas que comercializan equipamiento médico, como autoanalizadores de laboratorio o labo-

ratorios farmacéuticos, ofrezcan el programa que necesita el médico para su actividad diaria. Como es lógico, ante la falta de perspectiva de implantación de una solución corporativa, este tipo de soluciones se extienden, con un coste elevado y difícil integración posterior (Mazón *et al.,* 2000).

Altos costos asociados a la inversión inicial, altos costos de mantenimiento, incertidumbre sobre el retorno de la inversión y falta de fuentes de financiamiento (González y Luna, 2012)

Señala Carnicero Giménez (2004:280) «que en ocasiones se ofrecen sistemas con un coste inicial muy bajo, pero están pobremente diseñadas y los costes de formación y mantenimiento superan con rapidez los supuestos ahorros con relación a sistemas mejor desarrollados». No obstante lo anterior, deben tenerse en cuenta los costes del archivo de historias convencional, el espacio que necesita en los centros sanitarios, y los costes de personal que precisa para su funcionamiento. Sin embargo, como ocurre tantas veces con las tecnologías sanitarias, la informatización de la historia no supone una desaparición inmediata del archivo convencional, por lo que los costes aumentan. La informatización de la historia y su incorporación a un sistema integrado requiere una fuerte inversión que coincide en el tiempo con tensiones financieras de los sistemas sanitarios.

Los sistemas de salud-e redundan en una atención sanitaria de mayor calidad, pero requieren una inversión considerable que, aunque rentable hace difícil que se produzca una gran reducción de costes. Por ejemplo, la implantación de un sistema de imagen médica digital permite eliminar el uso de placas radiológicas, lo que a priori supone un gran ahorro económico, pero a cambio han de adquirirse y mantenerse sistemas de almacenamiento de alta capacidad y estaciones de diagnóstico con monitores de alta resolución, lo que requiere un desembolso económico importante. Una dificultad añadida en estos proyectos es la inmediatez de los costes frente a la demora en la apreciación de los beneficios, especialmente cuando estos son intangibles (Carnicero, Rojas y Blanco, 2014).

— *Dificultades culturales:* por otra parte, los clínicos consideran las TIC poco importantes tanto para la investigación como para la práctica médica. Los programas de informatización de

la historia clínica deben tener en cuenta las peculiaridades de la práctica clínica y facilitar las tareas del personal sanitario sin introducir actividades nuevas que no sean imprescindibles, deben facilitar el trabajo, no complicarlo, por ejemplo un error frecuente es orientar las soluciones informáticas hacia la explotación de datos para gestores, antes que considerarlas un instrumento más de la práctica clínica. En alguna ocasión proyectos importantes con fuerte dotación presupuestaria han fracasado por no tener cuestiones como estas (Carnicero, Rojas de la Escalera y Blanco, 2014).

La profesión médica, como el resto de profesiones sanitarias, incorpora continuamente innovaciones tecnológicas a su actividad diaria, se puede decir que se trata de una cualidad inherente a la profesión, la informática no tiene por qué ser diferente a otras tecnologías. Para las generaciones más jóvenes resulta más sencillo, porque la informática es un instrumento que forma parte de su vida incluso antes de acceder al mundo profesional (Falagán *et al.,* 2003).

— *Ausencia de estándares de aceptación universal:* no existe un estándar universalmente aceptado para la transferencia de datos clínicos, lo que supone que las diferentes aplicaciones no se comunican bien entre ellas y encarecen los costes de las conexiones; los estándares en muchas ocasiones pertenecen a entidades privadas y los costes de las licencias encarecen los procesos. A pesar de ello, los fabricantes de software tienden a ofrecer al mercado estándares abiertos e interoperables en tiempo real, porque esas son las demandas del mercado, los servicios Web y XML son ejemplos de esas tendencias. La irrupción de Internet como canal de comunicaciones ha tenido una gran influencia en este proceso (Moura, Indarte y De Faria, 2014).

— *Técnicos:* Falta de infraestructura informática adecuada (hardware, software y comunicaciones), insuficientes habilidades informáticas de los médicos o auxiliares; falta de capacitación y soporte; complejidad, limitaciones, obsolescencia e insuficientes opciones de personalización de los sistemas. La confiabilidad y alta disponibilidad son aspectos relevantes a tener en cuenta. Problemas asociados con la interoperabilidad e interco-

nexión con otros sistemas también constituyen una barrera importante.

— *Tiempo:* La selección, adquisición e implementación del sistema consume mucho tiempo. También se requiere tiempo para capacitar con relación a su uso, para ingresar los datos y para transcribir la información histórica contenida en historias clínicas de papel.

— *Psicológicos:* escepticismo y percepciones negativas con respecto a la HCE, necesidad de control de los cambios por parte de los profesionales y su percibida pérdida de autonomía.

— *Sociales:* incertidumbre sobre las empresas comercializadoras de los productos de HCE, falta de cooperación de todos los miembros del equipo de salud y la interferencia en la relación médico-paciente.

— *Legales:* aspectos relacionados con la privacidad y seguridad de la información.

— *Organizacionales:* el tamaño y el tipo de organización inciden. Los médicos que trabajan en organizaciones de mayor tamaño adoptan más las HCE y se observan mayores tasas de adopción en redes sanitarias que en consultorios individuales.

— *Manejo del cambio:* inadecuada transición en la cultura organizacional al migrar hacia la HCE, falta de incentivos, participación y de liderazgo (González y Luna, 2012).

— *Otras posibles desventajas:* para poder procesar los datos es necesario que estén codificados o estructurados, lo que contrasta con la necesidad de texto libre que tienen los clínicos; la historia clínica en papel puede ordenarse y cumplimentarse de forma que permite orientarse con facilidad, permite, por ejemplo, escribir en los márgenes, utilizar diferentes colores, tamaños de letra, flechas, símbolos y marcas que se entienden de forma intuitiva.

En la historia clínica electrónica es más fácil sentirse desorientado, la necesidad de ordenar, clasificar y codificar los datos precisa de grandes consensos que pueden retardar, y por lo tanto encarecer el desarrollo de la historia clínica informatizada. Como señala Carnicero Giménez (2004:283), «en el diseño de la historia clínica deben participar personas que estén familiarizadas y conozcan las tareas clíni-

cas y los datos que son relevantes»; los cambios que deban introducirse después son siempre muy caros. También resulta difícil y caro el procesado de imágenes médicas; en sentido contrario, la gran capacidad de procesar información que tienen los ordenadores puede conducir a acumular gran cantidad de datos que luego no se emplean y encarecen los procesos.

6.17 INFERENCIA DE UN SISTEMA DE INFORMACIÓN SANITARIO BASADO EN LA HISTORIA DE SALUD ELECTRÓNICA (HSE)

La historia de salud electrónica (HSE) no es una realidad ni una aplicación informática única, sino el resultado de la integración e interacción de varias fuentes de información, incluida la historia clínica electrónica que tiene como resultado un auténtico sistema de información de salud. Las consecuencias o inferencias de este sistema de información establecen un valor añadido sobre los sistemas convencionales en papel y no integrados, que se plasma en una serie de ventajas en las funciones de la historia clínica, inaccesibles a los sistemas convencionales.

Estas inferencias pueden ordenarse en tres niveles: vegetativo, operativo y epistemológico:

- *Nivel vegetativo:* que abarca funcionalidades que son consecuencia de la aplicación de la tecnología de una forma automática al sistema de información clínico. Las características básicas de los ordenadores son su capacidad en el manejo de datos, impensable por otros métodos, y su enorme posibilidad de almacenaje de información. Las ventajas de las TIC son las siguientes:
  - — Mejor gestión del archivo.
  - — Incremento de la accesibilidad, que tiene dos importantes aspectos la inmediatez y la concurrencia.
  - — Plasticidad, que se moldea de forma dinámica siguiendo los requerimientos de cada caso en particular.
  - — Mejora la confidencialidad, tiene mayores posibilidades de control de accesos.

— Dependencia tecnológica, los recursos y las tecnologías en que se apoya la HSE son diferentes de los tradicionales, pero no necesariamente mucho más caros.

— Vulnerabilidad física, las TIC cuentan con posibilidades para subsanar este inconveniente (Carnicero, Rojas de la Escalera y Blanco, 2014).

• *Nivel operativo:* cuando se aplica tecnología para resolver un fin concreto, precisa desarrollos específicos. La mayoría de las ventajas de este nivel requieren desarrollos específicos dirigidos a cubrir funcionalidades concretas. Las más evidentes son la integración de la información, la automatización de tareas repetitivas, la mejora de la actividad clínica, de los cuidados, de la gestión administrativa y de la comunicación.

— Integración de la información; se deben observar criterios y estándares sobre homogeneización de datos, modos de almacenamiento y protocolos de comunicación entre aplicaciones.

— Automatización de tareas reiterativas, emitir informes, recetas y correo en general.

— Manejo clínico y dispensación de cuidados, permiten disponer de una visión global del paciente, lo que supone una ventaja suficiente para evitar repeticiones de exploraciones y coordinar debidamente tratamientos y actuaciones.

— Gestión administrativa, debe facilitar la eficiencia de los procedimientos administrativos implicados en la salud de un individuo, evitando trámites innecesarios y reiterativos.

— Comunicación, la integración de toda la información de salud de una persona, que fluye entre los profesionales implicados en su mantenimiento y promoción (Carnicero Giménez *et al.*, 2003).

• *Nivel epistemológico:* son sistemas que utilizan el conocimiento explícito externo para lograr su fin. Parten de una información reglada y estructurada. No incorporan nueva evidencia procedente de la propia experiencia, sino a través de actualizaciones o puestas al día.

— Medicina basada en evidencia, integrar un sistema de ayuda a la toma de decisiones clínicas dentro de la historia clínica infor-

matizada, disminuye los errores médicos, aumenta la seguridad del paciente y disminuye la variabilidad clínica.

— Inteligencia artificial, los sistemas expertos de aplicación clínica deberían poder incorporar a sus bases de conocimientos las evidencias, pruebas, procedentes del conocimiento implícito de la HSE para poder utilizarlo, como experiencia propia, a la resolución de problemas (Indarti y Vero, 2014).

— Docencia e investigación, la historia clínica es una fuente de datos y un instrumento básico para la investigación biomédica, la formación de estudiantes y la formación médica continuada, puede constituir una fuente de información basada en la propia experiencia (Carnicero Giménez *et al.*, 2003).

6.18 DIAGNÓSTICO DEL ESTADO DE LA E-SALUD EN EUROPA

Se impulsó hace años el *eHelath Action Plan* 2012-2020 ideado como una hoja de ruta para lograr una atención sanitaria inteligente y sostenible para Europa. En concreto, el Plan presenta y consolida las acciones para disfrutar de las oportunidades que puede ofrecer la e-Salud. Además, describe el papel de la Unión Europea y alienta a los Estados miembros y a todos los actores implicados a trabajar juntos.

En concreto, esta iniciativa conjunta de la Vicepresidente de la Unión Europea y el Comisario de Sanidad y Consumo promueve cuatro (4) puntos clave:

— La mejora de la gestión de las enfermedades crónicas y pluripatológicas y la puesta en marcha de políticas para fortalecer la prevención eficaz de enfermedades y las prácticas de promoción de la salud.

— El aumento de la sostenibilidad y eficiencia de los sistemas sanitarios europeos mediante el desbloqueo de la innovación, posibilitando la atención centrada en el paciente y dando más poder al ciudadano, además del fomento de cambios en las organizaciones sanitarias.

— El impulso de la asistencia sanitaria transfronteriza, la seguridad sanitaria, la universalidad y la equidad.

— La mejora de las condiciones legales y del mercado para el desarrollo de productos de e-Salud.

El Plan de Acción de e-Salud 2012-2010 marca objetivos operacionales para superar obstáculos que frenen el uso de soluciones digitales dentro de la Unión Europea, y que por tanto, supongan barreras a la implantación de la e-Salud en los países de la Unión Europea. Se puede resumir los objetivos en 4:

1. Conseguir una mayor interoperabilidad de los servicios de e-Salud, creando un marco de interoperabilidad en e-Salud basado en los resultados de la investigación, pilotos y proyectos de investigación.

2. Apoyar la I+D+i y la competitividad en e-Salud, durante el periodo 2014-2020, los proyectos de I+D+i en este sector recibirán financiación del programa público europeo Horizonte 2020, dentro del área «Salud, cambio demográfico y bienestar».

3. Facilitar y garantizar el amplio despliegue de la e-Salud, impulsando acciones para mejorar las capacidades digitales de ciudadanos, pacientes y profesionales de la salud. Además, indica que a partir de 2014 se pondrá a disposición de los interesados una serie de indicadores para medir el valor añadido y los beneficios de la e-Salud.

4. Promover el diálogo político y la cooperación internacional en e-Salud a nivel mundial, ya que tanto la Organización Mundial de la Salud (OMS), la Organización para la Cooperación y el Desarrollo Económico (OCDE) como otros entes internacionales insisten en la importancia de proponer soluciones a las cuestiones relacionadas con la e-Salud.

El Consejo Europeo instó al ejercicio del liderazgo político y a integrar la e-Salud en las políticas sanitarias con el objetivo de desarrollar servicios de e-Salud en respuesta a las nuevas necesidades de la sanidad pública.

Durante la Presidencia española de la Unión Europea en el primer semestre de 2010, tuvo lugar en Granada la Cumbre de los Ministros de Telecomunicaciones y Sociedad de la Información. Esta cumbre ha dado lugar a la que desde entonces se conoce como «*La Estrategia de Granada*»; de esta reunión surgió la nueva estrategia europea en materia TIC para el periodo 2010-2020, que viene a remplazar a la iniciativa de Lisboa i2010. Esta estrategia abarca todo lo concerniente

al desarrollo de las bases de la Europa Digital que está por construir, y establece cinco (5) grandes ejes de actuación:

1. Las infraestructuras.
2. El uso avanzado de Internet.
3. La carta europea de derechos de los usuarios.
4. El desarrollo de servicios y contenidos digitales.
5. El fortalecimiento del sector de las tecnologías de la información.

En la *Estrategia de Granada* se plantearon y aprobaron una serie de cuestiones relativas a la *eHealth* o e-Salud. Las cuatro (4) líneas estratégicas que se proponen en este ámbito son las siguientes:

1. Introducir una visión global para una política de Sanidad Digital integrada dentro de la Agenda Digital Europea pos 2010.
2. Impulsar un nuevo Plan de Acción de e-Salud.
3. Promocionar e incentivar acuerdos ministeriales que integren las políticas de Sanidad Digital en sus propias agendas.
4. Implantar mecanismos reforzados de gobierno en estas iniciativas.

Los objetivos propuestos y aceptados en el marco de esta estrategia son los siguientes:

— *Sanidad Digital para una Europa más sana:* garantizando la calidad y continuidad de los cuidados en el Espacio de Salud Europeo.

— *Sanidad Digital para el crecimiento sostenible y la cohesión:* el sector Sanidad Digital como generador de cohesión social y riqueza en términos de empleo, innovación y desarrollo económico.

— *Sanidad Digital como sector industrial:* generar las condiciones favorables para facilitar el despegue del mercado e-Salud europeo en aquellas áreas con mayor potencial de crecimiento.

— *Sanidad Digital para la innovación y el cambio social:* innovación tecnológica y creatividad para transformar los procesos de atención sanitaria, mejorar la calidad de vida, trabajo y las

condiciones de envejecimiento, poniendo el foco en la prevención de enfermedades y la gestión de la cronicidad.

— *Sanidad Digital para la capacitación de los ciudadanos:* la Sanidad Digital puede jugar un papel clave para incrementar la participación de los ciudadanos en el cuidado de su salud.

— *Uso de la tecnología* para identificar eficiencias y áreas de mejora de las políticas sanitarias y medir resultados de salud.

Podemos estimar que, desde el punto de vista del paciente, las nuevas tecnologías permiten:

— Promover una intervención activa e informada del ciudadano en el cuidado de su salud, así como un mejor control de sus dolencias y tratamientos asociados.

— Multiplicar los canales de acceso a la información sobre temas de salud. Junto a los canales tradicionales (médico, farmacéutico, etc.), los ciudadanos acuden a las redes sociales e Internet para buscar información de salud.

— Mejorar la seguridad y calidad de la atención que reciben los ciudadanos gracias a un mejor acceso de los profesionales a la información clínica del paciente.

— Favorecer el desarrollo de nuevos modelos de atención que permitan la permanencia del paciente en su domicilio evitando desplazamientos innecesarios a los centros y garantizando una atención de calidad (ONTSI, 2012).

Para contribuir en la mejora de los servicios públicos, la Comisión Europea publica periódicamente análisis comparativos con datos de los Estados miembros. En el caso de la sanidad, se acaban de hacer públicos los resultados de dos (2) encuestas en el ámbito europeo sobre TIC y salud que permiten hacer el seguimiento del desarrollo del Plan de Acción de e-Salud 2012-2020 y de la Estrategia Europa 2010.

El primero de estos estudios es el proyecto *European Hospital Survey: Benchmarking Deployment of e-Health services* (2012-2013), llevado a cabo por el Instituto de Prospectiva Tecnológica (IPTS), uno de los siete (7) centros de investigación de la Comisión Europea. El objetivo ha sido analizar el desarrollo de la e-Salud en los hospitales de agudos, como institución clave de los sistemas sanitarios, con el fin de identificar tendencias. Para llevar a cabo el proyecto, se han reali-

zado más de 1.000 entrevistas a directores médicos y *Chief Information Officers* (CIO) de más de 900 hospitales de 30 países.

Según los resultados, el desarrollo de la e-Salud en los hospitales europeos ha crecido de un 39% a un 42% en el periodo 2010-2013. Los países con unos índices más altos de desarrollo de la salud electrónica son Dinamarca (66 %), Estonia (63 %), Suecia y Finlandia (ambos con un 62 %). Además, las diferencias entre los países en los que más se ha adoptado la e-Salud –la gran mayoría, países nórdicos– y los países menos adelantados (Europa del Este y Grecia, Letonia y Lituania) han disminuido.

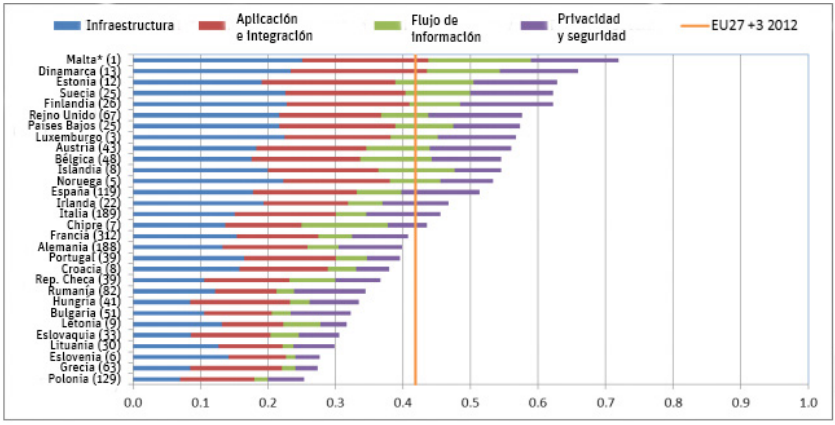

Figura 18. Diagnóstico del estado de la e-Salud en Europa

Fuente: Comisión Europea «Desarrollo de la e-Salud en 2012 por país». El número en paréntesis al lado de cada país indica el número de hospitales que ha participado en la encuesta de la Comisión Europea. El asterisco de Malta indica que sólo un hospital ha participado en la encuesta y los resultados para este país no son representativos, según los autores.

Sin embargo, no todos los hospitales tienen a su alcance soluciones avanzadas de e-Salud, aunque cuando sí se disponen de ellas, su uso es mayoritario. Por ejemplo, el *Picture Archiving and Communications System* - PACS radiológico sólo se puede encontrar por ahora en el 53 % de los hospitales europeos, donde es utilizado por el 92 % de sus profesionales.

Los resultados del estudio sugieren que la conectividad es uno de los temas pendientes de los hospitales, ya que la mayoría de los cen-

tros no comparten información. En cuanto a la inversión, el 63% de los hospitales europeos dedica menos de un 3% de su presupuesto anual a las TIC. Algunos hospitales, más de la mitad de la muestra (57%), disponen de un Plan Estratégico en TIC, algo que resulta más habitual en los países de la Europa Occidental.

En cuanto a la informatización de las historias clínicas, los Países Bajos llevan la avanzada en esta cuestión (las EHR se han desplegado en el 83,2% de los centros). Les siguen Dinamarca (80,6%) y Reino Unido (80,5%). Por otra parte, el 85% de los hospitales estudiados dispone de unas normas muy claras en cuanto al acceso de los pacientes a sus datos médicos, aunque sólo un 9% del total de centros de la Unión Europea dan accesibilidad a los ciudadanos y muchos de ellos sólo permiten el acceso parcial a los datos online. Dinamarca, Finlandia, Noruega y Croacia son los más accesibles. Esto frena una mayor implicación del paciente en la autogestión de su salud.

El segundo estudio que ha publicado la Comisión Europea corresponde al proyecto *Benchmarking Deployment of Health among General Practitioners 2013*, centrado en el uso de las TIC por los médicos generalistas. Los resultados demuestran que las aplicaciones de e-Salud están cada vez más presentes en las prácticas médicas.

A raíz de las entrevistas a 9.196 médicos de 31 países (de la UE27, Croacia, Islandia, Noruega y Turquía) se han identificado diferencias significativas en la disponibilidad de soluciones en Europa. También se señalan las áreas a mejorar, en concreto la prescripción electrónica, la telemedicina o la interoperabilidad transfronteriza. A pesar de todo, se constata un resultado positivo en todos los países: hay un ordenador con conexión a Internet en casi todas las consultas y un alto porcentaje de médicos de familia utilizan la red para su formación continua.

El 93% de los médicos tiene acceso a servicios básicos de Historia Médica Electrónica (EHR). Sin embargo, el estudio identifica la falta de desarrollo de las características más avanzadas a nivel europeo. Por otra parte, este tipo de servicios se están usando mayoritariamente para almacenar informes y datos más que con fines clínicos como, por ejemplo, la consulta en línea. En total, solo un 10% de los médicos generalistas europeos está usando en la actualidad las posibilidades de consulta en línea.

La adopción de la e-Salud está influenciada por el nivel de desarrollo del país, pero también por las características individuales y aptitu-

des de los médicos, aseguran los autores del informe. De hecho, la gran mayoría de los profesionales encuestados hace más énfasis en las barreras que en los beneficios de la e-Salud. Los obstáculos a los que más se han referido son la falta de incentivos financieros y recursos (79%), las insuficientes competencias informáticas (72%), la falta de interoperabilidad (73%) y la inexistencia de un marco de regulación en cuanto a la confidencialidad y a la privacidad para los pacientes (71%).

El Comisario Europeo de Salud, Tonio Borg, ha puesto de manifiesto que «los Estados miembros que más uso hacen de historias clínicas electrónicas y recetas electrónicas deben ser fuente de inspiración para todos» (TicSalut, 2013).

6.19 ADOPCIÓN DE LA HISTORIA CLÍNICA ELECTRÓNICA EN DIFERENTES PAÍSES DEL MUNDO

A pesar del amplio consenso que existe sobre los beneficios de las historias clínicas electrónicas (HCE), su tasa de adopción es dispar en el mundo entero. Se observan muy buenas tasas de adopción en Australia, Holanda, el Reino Unido y Nueva Zelanda, así como en España y países nórdicos. En los Estados Unidos, la tasa de adopción es baja, tanto en el nivel ambulatorio de atención como en el ámbito de pacientes internados, mostrando un leve repunte en este nivel de atención luego de la implementación de incentivos fiscales por parte del gobierno. Dichos incentivos son otorgados según criterios de uso significativo de las funcionalidades de las HCE (Blumenthal y Tavenner, 2010).

Una muy buena herramienta para el análisis y clasificación de las funcionalidades de las historias clínicas electrónicas alcanzadas por las instituciones de salud es el *Healthcare Information and Management Systems Society Adoption Model* (HIMSS *Adoption Model*). Por medio de esta clasificación de ocho (8) niveles funcionales es posible cuantificar el grado de avance con relación a las HCE de las organizaciones de salud de un país. En la encuesta realizada por dicha organización, en el año 2010 y en los Estados Unidos, solo el 20% de las instituciones encuestadas se encontraba en nivel 4 o superior (González y Luna, 2012).

Tabla 7. Características de las funcionalidades alcanzadas

Nivel	Características de las funcionalidades alcanzadas
7	— La organización no usa papeles en el contexto del uso de una HCE.
6	— Implementación del ingreso de datos por medio de plantillas en al menos un área de servicios. — Posee un sistema de radiología digital con disponibilidad de imágenes en la HCE. — La información clínica puede ser compartida por medio de estándares de intercambio de datos. — Este estadio permite a las organizaciones intercambiar efectivamente los datos clínicos de sus pacientes con otras organizaciones. — Posee bases de información que posibilitan la agregación de datos clínicos tanto en la captura como en el análisis. — Utiliza técnicas de inteligencia de negocios como *data warehouse* y minería de datos *(data mining)* para capturar y analizar los datos. — Mejora los protocolos de atención por medio de soporte para la toma de decisiones.
5	— Sistema de prescripción electrónica completamente implementado en al menos un servicio clínico. — Cuenta con funcionalidades de autoidentificación por código de barras o radiofrecuencia en el contexto de un sistema de farmacia integrado para maximizar la seguridad de los pacientes.
4	— Sistema estructurado de órdenes médicas implementado y almacenamiento de los reportes en un repositorio de datos clínicos común. — Segundo nivel de soporte para la toma de decisiones relacionado con protocolos de medicación implementado.
3	— Sistema de documentación clínica implementado (por ejemplo, signos vitales, notas de enfermería, balance y prescripciones médicas) en al menos un servicio médico. — Primer nivel de sistema de soporte para la toma de decisiones implementado en cuanto al chequeo de errores en el ingreso de las prescripciones (por ejemplo, detección de interacciones droga-droga, droga-enfermedad, droga-laboratorio, droga-alimentos, duplicaciones y otros). — Algún nivel de acceso a radiología digital por medio de redes seguras o intranet institucional pero no integrado en la HCE.
2	— Envío de reportes de efectores de exámenes complementarios a un repositorio de datos clínicos común que permite el acceso de los profesionales. — Soporte de toma de decisiones rudimentario (chequeo de duplicaciones). — Utilización de terminologías clínicas controladas. — La información escrita sobre imágenes se relaciona con el repositorio de datos clínicos (no las imágenes).

1	— Sistemas departamentales instalados (laboratorio, radiología y farmacia, entre otros).
0	— Sistemas departamentales no instalados.

Fuente: González y Luna (2012: 92)

6.20 SERVICIOS DE HISTORIA CLÍNICA PERSONAL EN LÍNEA

Una *historia clínica personal* se define como una aplicación electrónica mediante la cual una persona puede acceder, gestionar y compartir la información relativa a su salud en un entorno privado, seguro y confidencial (Markle Foundation, 2003 y Tang y otros, 2006).

La creciente movilidad de los ciudadanos ha suscitado mayor preocupación por la disponibilidad de su información clínica personal, en previsión de que puedan necesitar la asistencia de un servicio de salud distinto de aquel al que están adscritos. Aunque existen proyectos para la creación de espacios de interoperabilidad en materia de salud a escala nacional e internacional (Abad y Carnicero, 2012), la implantación de diferentes servicios TIC ha llevado a algunos pacientes a buscar soluciones de historia clínica personal por iniciativa propia. Inicialmente se planteó el uso de dispositivos portátiles de almacenamiento de datos, como soportes ópticos (CD y DVD), tarjetas chip (opción que algunos servicios de salud valoran), o unidades de disco con conexión USB. Los principales inconvenientes de estos dispositivos son la dificultad para actualizar los datos y el riesgo de daño, extravío o robo. Aunque existen mecanismos para proteger la confidencialidad de los datos almacenados, como las contraseñas de acceso o la encriptación de la información, persiste el problema de la disponibilidad, que es precisamente la utilidad buscada por el paciente al adoptar este tipo de solución.

En la actualidad hay una clara preferencia por soluciones basadas en entornos web, que eliminan la necesidad de transportar personalmente la información, sin merma alguna de la disponibilidad, debido al altísimo grado de conectividad de Internet. Además, algunas de estas aplicaciones pueden integrarse con otros sistemas de intercambio de datos, y también son accesibles desde dispositivos móviles (Tang y otros, 2006).

A pesar de la amplia oferta existente, el uso de estos servicios es aún minoritario, debido principalmente a la preocupación de los pacientes por la confidencialidad de sus datos. De hecho, a mediados de 2011 *Google* hizo pública su decisión de cerrar el servicio *Google Health* a partir del 1.º de enero de 2012, aduciendo una escasa penetración del servicio en el mercado. El desmantelamiento del portal culminó el 1.º de enero de 2013 con la eliminación de todos los datos existentes, pero hasta ese momento se permitió a los usuarios descargar los datos almacenados o transferirlos a aplicaciones similares, como *Microsoft HealthVault*, opción expresamente recomendada por el propio *Google*.

El recelo de los usuarios puede haber sido provocado en parte por las dudas sobre la aplicabilidad de la legislación vigente. En los términos de uso de *Google Health*, la compañía consideraba que la normativa estadounidense sobre protección de la intimidad en entornos de salud no era aplicable, y lo mismo sucede en el caso de *Microsoft HealthVault*. El debate sobre la posible existencia de un vacío legal respecto del almacenamiento de datos clínicos por parte de empresas tecnológicas ha podido provocar cierta desconfianza en el mercado estadounidense que sería mucho más proclive a este tipo de soluciones individuales ante la ausencia de un sistema público de salud, tanto estatal como federal (Martínez y Rojas de la Escalera, 2014).

En el cuadro Historia Clínica Personal se recogen las principales características de algunas de las soluciones más conocidas.

Tabla 8. Historia Clínica Personal: Características de algunas soluciones comerciales

Nombre comercial	Funcionalidades y servicios
Google Health (2008-2013)	Información registrada: • Estado general de salud. • Tratamiento farmacéutico activo. • Alergias. • Resultados de laboratorio. Otros servicios: • Generación de historia clínica resumida. • Alertas de posibles interacciones medicamentosas y reacciones alérgicas.

Microsoft HealthVault (2007) www.healthvault.com www.healthvault.co.uk	Información registrada: • Historia clínica. • Imagen médica en formato DICOM (Digital Imaging and Communication in Medicine). Otros servicios: • Integración con sensores para el registro de constantes vitales. • Posibilidad de permitir el acceso de familiares y profesionales. • Compatibilidad con estándares CCD (continuity of care document), y CCR (continuity of care register), para intercambio de datos.
World Medical Card (1998) World Medical Center, Noruega www.wmc-card.com	Información registrada: • Historia clínica. • Tratamiento farmacéutico activo. • Alergias. • Vacunas. • Personas de contacto en caso de emergencia. • Documentos cargados personalmente por el paciente. Otros servicios: • Acceso desde dispositivos móviles. • Tarjeta chip con historia clínica resumida.
Dossia (2009) Consorcio AT&T, Intel y otros www.dossia.org	Información registrada: • Datos procedentes de registros médicos y de compañías aseguradoras. • Anotaciones personales del paciente.

Fuente: Martínez y Rojas de la Escalera (2014:270)

6.21 LAS REDES SOCIALES

Durante muchos años, la rápida implantación de las TIC en el sector financiero se usó habitualmente como estímulo para promover el desarrollo de la e-salud. En la actualidad es frecuente escuchar referencias a las redes sociales como el nuevo «ejemplo a seguir», e incluso algunas muestras de extrañeza por el hecho de que no se empleen con fines asistenciales. Teniendo en cuenta el grado de penetración de estas redes, probablemente superior al de cualquier otra herramienta de comunicación, es comprensible que se planteen ideas de este tipo.

Sin embargo, si en el primer caso se puede argumentar que el sector de la salud es comparativamente mucho más complejo que el financiero, en el segundo se puede afirmar que las prestaciones de las redes sociales no se ajustan a las necesidades asistenciales, sobre todo en materia de confidencialidad de la información.

En líneas generales, estos servicios permiten a los usuarios enviar mensajes, compartir archivos y acceder a aplicaciones en línea. Para esto, el usuario debe crear un perfil con datos personales básicos y, lógicamente, cargar la información que desee compartir.

La gestión de esta información por parte del proveedor es la principal fuente de dudas y quejas de los usuarios, que reclaman una mayor claridad y transparencia durante este proceso. Tal preocupación es especialmente patente en el caso de los usuarios que deciden darse de baja del servicio, porque albergan dudas sobre la eliminación definitiva de sus datos y temen su posible uso ilícito por parte del proveedor. La ausencia de un marco legal específico y la escala internacional de estos servicios contribuyen a complicar aún más la situación.

No obstante, existen algunas experiencias positivas de uso en relación con la salud, como el caso de *PatientsLikeMe*, una red social específicamente diseñada para que los pacientes puedan establecer contacto entre ellos y apoyarse mutuamente, pero que en ningún caso ofrece asesoramiento médico. Tras comenzar su actividad en 2006 con un grupo de pacientes de esclerosis lateral amiotrófica, se añadieron progresivamente grupos correspondientes a otras enfermedades, como epilepsia, SIDA, fibromialgia o Parkinson, y también grupos de trasplante de órganos. Desde abril de 2011 el servicio está disponible para todo tipo de pacientes y en septiembre de 2015 se había llegado a un total de 350.000[83] usuarios.

---

[83] PatientsLikeMe (2015) [en línea]: https://www.patientslikeme.com/ [Consulta: 15/06/2015]

Figura 19. Vista del sitio web patientslikeme

Fuente de elaboración: patientslikeme.

Los pacientes son libres de compartir información sobre los tratamientos administrados y los resultados conseguidos, pero la política de privacidad del portal alerta expresamente sobre los riesgos que ello puede suponer: «*PatientsLikeMe no puede acreditar la identidad de cualquier otro miembro que pueda interactuar con el usuario durante el uso del sitio o que pueda acceder a los datos compartidos por el usuario. Adicionalmente, no podemos garantizar la autenticidad de los datos personales aportados por los miembros […] Los usuarios deben comprender que cualquier persona puede registrarse en PatientsLikeMe y visualizar los datos compartidos en el sistema. Si usted está leyendo esta política de privacidad porque tiene acceso a la información personal de un usuario del sitio, le urgimos a reconocer y cumplir con su responsabilidad de proteger la identidad de dicha persona*».

Aunque el nivel de satisfacción de los usuarios es elevado y la imagen pública del portal es bastante positiva, hay constancia de algunos intentos ilícitos de recabar información por parte de terceros. Sucesos como estos demuestran que las redes sociales están diseñadas para compartir datos, pero no para protegerlos, puesto que tanto el proveedor como los demás usuarios pueden copiarlos y utilizarlos. Es más, en el caso del proveedor es un hecho reconocido que la explotación de esta información es la base de su modelo de negocio. Por lo tanto, el usuario tiene que ser consciente de ello y extremar las pre-

cauciones a la hora de hacer uso de estos servicios, que bajo ningún concepto deben ser empleados como repositorios de información clínica (González y Luna 2014). En el caso de España, solo un 12,8% de los internautas utiliza las redes sociales para consultar información relacionada con la salud, siendo su nivel de confianza de apenas un 7,1% (ONTSI, 2012).

6.22 OTROS USOS DE INTERNET PARA LA SALUD

Desde su aparición, la oferta de contenidos y servicios de Internet no ha dejado de crecer, a la par con sus facilidades de conexión. En España, un 48,3% de los internautas utiliza Internet como fuente de información sobre salud (ONTSI, 2012). Como consecuencia, cada vez es mayor el número de pacientes que acuden a la consulta médica después de haber buscado información en la red (Gabarrón y Fernández-Luque, 2012). Algunos de ellos llegan al extremo de autodiagnosticarse y reclamar al médico la prescripción de un tratamiento determinado, situación que varios profesionales han comparado con la de atender a un cliente en un supermercado.

La disponibilidad de una cantidad excesiva de información, aunque esta sea correcta, impide distinguir los datos relevantes de aquellos que no lo son, causando por lo tanto la generación de ideas equivocadas y la toma de decisiones erróneas. Actualmente se utiliza también el término «*infoxicación*», resultado de combinar información e intoxicación. Aunque disponer de un mayor acceso a la información sea a priori un hecho positivo, es necesario recordar que la utilidad de los datos depende no solo de su cantidad, sino también de su calidad, y que la generación de conocimiento no es una consecuencia automática de la disponibilidad de información, sino que está supeditada a su correcta interpretación.

Buen ejemplo de ello es el hecho de que los distintos proyectos institucionales de interoperabilidad en el área de la salud cuenten con una historia clínica resumida (Etreros, 2009 y Abad y Carnicero, 2012) de modo que los profesionales puedan acceder con la mayor rapidez posible a los datos más importantes. En estudios recientes se muestra que, desde el punto de vista de los internautas españoles, las dos barreras más importantes para el uso de Internet como fuente de información sobre salud son precisamente la fiabilidad de los da-

tos (54,4%) y el riesgo de su interpretación errónea (28,7%), lo que contribuye a situar su nivel de confianza en unos escasos 3,85 puntos sobre 10 (ONTSI, 2012).

El hecho de que las redes sociales online sean accesibles a cada vez un mayor número de personas convierte a este medio de comunicación en una poderosa herramienta para divulgar y educar a los usuarios en temas sanitarios de interés general. En todas las redes sociales los vídeos se están convirtiendo en un recurso en pleno auge, y aunque originalmente en su inmensa mayoría eran vídeos caseros creados por los propios usuarios, mostrando experiencias personales o dando consejos a otros pacientes, hoy día existe un creciente número de instituciones u organismos oficiales que están creando canales de comunicación 2.0 y utilizan estas potentes plataformas para divulgar información sobre salud.

La difusión de información sobre salud en plataformas de vídeo online presenta ventajas indiscutibles, como su bajo costo, su enorme potencial de hacer llegar información rápidamente a un amplio sector de la población o el hecho de facilitar la interacción con los usuarios, pero también tiene desventajas, ya que en muchos casos no puede identificarse al autor de los vídeos, no se citan fuentes, se muestran opiniones personales como si fueran hechos científicos o algunos aspectos quedan sin respuesta, por lo que puede ser difícil para el usuario valorar la calidad de sus contenidos.

Actualmente se tiene varios ejemplos de grandes instituciones sanitarias de reconocido prestigio que utilizan plataformas de vídeos sociales para comunicarse con pacientes, entre las que se pueden destacar dos organizaciones de salud americanas, la *Food and Drugs Administration* (FDA) y los *Centers for Control and Prevention of Diseases* (CDC). En Europa se cuenta con algunos ejemplos similares, como el *National Health Service* (NHS) de Reino Unido y el *Instituto Karolinska* de Suecia, que están utilizando *YouTube* y *Facebook* para comunicarse con el público. En España se puede mencionar al Ministerio de Sanidad y Política Social, que ya ha publicado cerca de un centenar de vídeos online, y algunos hospitales, fundaciones y particulares también lo están empezando a hacer.

Es crucial que los organismos y los individuos que quieran usar vídeos online para promover la salud sigan las guías y recomendacio-

nes al respecto (como la de Andalucía[84]). El contenido es clave, pero si el mensaje no es claro y atractivo, difícilmente llegará a la población objetivo.

Sin embargo, para que los contenidos sean realmente accesibles se debe tener en cuenta a los usuarios con limitaciones sensoriales o cognitivas. En el caso de los vídeos online, el uso de subtítulos facilitaría el acceso a personas con problemas auditivos, y un diseño más sencillo, con menos enlaces y botones, facilitaría el acceso a las personas con problemas cognitivos o menos familiarizadas con Internet. Finalmente, hay que insistir en que todo lo que hay en la red no es bueno y en que queda mucho por hacer, por parte de las grandes instituciones y de los organismos sanitarios, a la hora de educar, dar respuestas a temas de salud o abrir vías de comunicación más directas con los usuarios (Gabarrón y Fernández – Luque, 2012).

6.23 SALUD MÓVIL

Según un informe del Banco Mundial de julio 2012, aproximadamente un 75% de la población mundial tiene acceso a un celular y se estima que existen más de 6.000.000.000 de celulares en el mundo, de los cuales 5.000.000.000 corresponden a países en desarrollo (Banco Mundial, 2012). El uso de los teléfonos móviles ha tenido un efecto considerable en los países en desarrollo debido a sus características: portabilidad, ubicuidad, comunicación en tiempo real, y posibi-

---

[84] Este acceso masivo a la información sobre salud en internet ha conllevado de manera paralela un aumento de páginas web sobre esta temática, de ahí que desde la Agencia de Calidad Sanitaria de Andalucía, ya en 2005, se detectara la necesidad de poner en marcha un instrumento que pudiera validar la calidad de las mismas. Este instrumento, enmarcado en los programas de certificación de la calidad de los diferentes elementos que conforman los sistemas sanitarios, es el Manual de Estándares de Páginas Web Sanitarias, encargado de facilitar la certificación de páginas web de instituciones, colectivos científicos y ciudadanos, etc., cuyo contenido fundamental sean los temas de salud. Agencia de Calidad Sanitaria de Andalucía (2015). *«Certificación de webs y blogs sanitarios»* [en línea]: http://www.juntadeandalucia.es/agenciadecalidadsanitaria/certificacion-acsa/certificacion-de-webs-y-blogs-sanitarios/ [Consulta: 25/06/2015].

lidad de acceso a información y servicios. Las personas usan sus celulares todos los días, los llevan a todas partes y los personalizan a su gusto, por lo que el usuario mantiene una especie de relación íntima con un dispositivo ubicuo (Klasnja y Pratt, 2012).

El incremento del uso de tecnologías de comunicaciones móviles, especialmente intenso en los últimos años, ha tenido un impacto en el ámbito sanitario con la aparición de la salud móvil, que consiste en el uso de dispositivos móviles en la práctica médica y la salud pública. La alta penetración de este tipo de dispositivos en el mundo puede suponer una gran oportunidad para fortalecer los sistemas de información sanitaria y transformar los sistemas de salud, aprovechando ventajas como la portabilidad, la comunicación en tiempo real y el acceso a datos y servicios.

La aplicación de la salud móvil en atención primaria contribuye, por lo tanto, a mejorar la accesibilidad de la asistencia (Curioso, 2014). Existen oportunidades como las siguientes:

— *Comunicación entre personas y servicios de salud:* centrales de llamadas telefónicas de ayuda o soporte en materia de salud para dar asesoramiento profesional al paciente en temas específicos, como salud sexual y reproductiva, enfermedades infecciosas como el VIH, salud mental, promoción de la salud, emergencias y desastres.

  En el informe *New horizons for health through mobile technologies* se muestra que en más del 40% de los países miembros de la Organización Mundial de la Salud se han establecido centrales de llamadas de ayuda o soporte relacionadas con temas de salud (OMS, 2011). Dichas centrales funcionan en muchos casos las 24 horas del día y todos los días de la semana. Su operación y gestión pueden estar en manos públicas o privadas, aunque la mayoría de estos servicios son privados y a los clientes se les cobra por su uso; en general, los cobros se hacen mediante convenios con las compañías telefónicas operadoras. En algunos países, como Finlandia, dichas centrales están vinculadas a historias clínicas electrónicas.

— *Comunicación entre servicios de salud y personas:* control de la adherencia al tratamiento, recordatorios de citas de consultas o exámenes clínicos, y campañas de promoción de la salud[85].

Mediante mensajes de texto o de voz se puede recordar a los pacientes la toma de medicinas y darles información relacionada con su enfermedad. Este sistema de recordatorios se está implementando en todo el mundo para atender condiciones crónicas: asma, diabetes, hipertensión, enfermedad pulmonar obstructiva crónica, tuberculosis y VIH/SIDA, entre otras (Riley y otros, 2011). En general, existen más programas recordatorios basados en mensajes de texto, debido a su bajo costo y a lo sucinto del mensaje, sin necesidad de hablar. Sin embargo, en países como Bután, Colombia, el Congo y Sierra Leona se han implementado programas recordatorios basados en mensajes de voz. En el mismo informe se muestra que aproximadamente en un 35% de los países miembros de la OMS se han implementado iniciativas encaminadas a mejorar la adherencia al tratamiento; destacan los países miembros del sudeste de Asia, un 50% de los cuales tiene en marcha este tipo de servicios (OMS, 2011).

En Bolivia se ha desarrollado Dr. Hora, un servicio gratuito que permite a los pacientes buscar, comparar y encontrar un

---

[85] Tres aplicaciones de un total de 198 ganaron el concurso realizado en alianza con la Fundación Trabajo Empresa. Las aplicaciones ganadoras en sus versiones 1.0 son *Healthy Memory* del chuquisaqueño Said Pérez, Reciclapp del cruceño Henry Saucedo y Trámites del paceño Gudnar Huanca. Pérez será además uno de los dos emprendedores bolivianos que el 21 de noviembre de 2014 representarán al país en el *«Get in the Ring»*, un certamen que invita a proyectistas de todo el mundo a presentar en Rotterdam (Holanda) sus planes de negocio a inversores de varios países y le ofrece al ganador una inversión de $us 1,28 millones. *Healthy Memory* (Memoria Saludable) conecta virtualmente y en tiempo real al médico con el paciente y permite a los profesionales en salud controlar la medicación de los enfermos. La app servirá también para recibir recetas, notificaciones e identificará las farmacias más próximas con los medicamentos que el paciente necesite. La Razón (2014), *«Bolivia exhibirá ante el mundo una appmóvil»* Periódico de circulación nacional [en línea]: http://www.la-razon.com/suplementos/financiero/Bolivia-exhibira-mundo-app-movil-financiero_0_2136986375.html [Consulta: 18/06/2015].

doctor o dentista en su ciudad, consultar su disponibilidad y hacer una cita al instante mediante el sitio web www.drhora.com) y una aplicación para móvil en cualquier momento 24/7. La aplicación es una herramienta para doctores y dentistas; la misma les permite gestionar de manera más eficiente la agenda de su consultorio y publicitar sus servicios en el sitio web logrando captar nuevos clientes. Este emprendimiento fue presentado en Emprendeideas 2014[86] impulsado por la Sociedad Boliviana de Cemento (SOBOCE) y salió ganador a nivel del Departamento de Tarija.

Los mensajes, de texto o de voz, se envían a los pacientes para recordarles una cita relacionada con la salud, como una consulta con un médico u otro profesional de la salud, una vacunación o una notificación de resultados de laboratorio, y también para programar una cita (Chen y otros, 2011).

El uso de mensajería de texto vía celulares a un costo reducido ha demostrado su efectividad, y puede utilizarse para motivar a los individuos y promover estilos de vida saludable mediante programas y campañas de salud, incluido el fomento de la actividad física (Curioso, 2014).

— *Comunicación entre profesionales de la salud:* telemedicina.

La telemedicina móvil puede ser definida como la comunicación o consulta entre profesionales de la salud acerca de pacientes mediante el uso de un teléfono móvil y sus funcionalidades de voz, texto, datos, imágenes o video (OMS, 2011).

En asistencia primaria también puede aplicarse en otras situaciones, como manejo de enfermedades crónicas de pacientes que viven en casa. En muchos países en desarrollo, la falta de recursos humanos es una barrera importante en el acceso de los pacientes a tratamiento o manejo especializado. Las tecnologías móviles son una oportunidad de acortar estas brechas al conectar a profesionales de la salud y pacientes con el

---

86 Bolivia Emprende (2014), «*SOBOCE premió a 61 ganadores de concurso Emprendeideas*» [en línea]: http://boliviaemprende.com/noticias/soboce-premio-61-ganadores-de-concurso [Consulta: 20/06/2015].

objetivo de mejorar la calidad de vida y reducir las referencias innecesarias.

En diversos estudios, como los realizados en la provincia china de Taiwán se ha evaluado la factibilidad de diagnosticar a distancia lesiones de tejidos blandos mediante la cámara de un teléfono móvil, o de transmitir imágenes para el diagnóstico remoto de la tuberculosis (Zimic y otros, 2009). Otros investigadores han evaluado la transmisión de imágenes vía teléfonos celulares usando el sistema de mensajería multimedia (MMS, por sus siglas en inglés), e incluso teléfonos celulares inteligentes, como iPhones. Las limitaciones a los sistemas de telemedicina móviles incluyen el tamaño de la pantalla del teléfono, la calidad de la imagen y la capacidad de la conexión a la red para transmitir datos, especialmente videos (Curioso, 2014).

— *Monitoreo de salud y vigilancia:* encuestas y vigilancia de eventos, monitoreo de pacientes y demás.

En el contexto de la salud móvil, la monitorización de pacientes se define como el uso de la tecnología para manejar, monitorizar y tratar la condición de un paciente (diabético o hipertenso, por ejemplo), a distancia (OMS, 2011). Frecuentemente se usan sensores remotos instalados en los hogares o cámaras conectadas a dispositivos móviles para facilitar la transmisión de datos a un proveedor de salud en asistencia primaria. De esta forma, mediante sensores se puede medir y monitorear remotamente presión arterial, peso, glucosa en la sangre y actividad eléctrica del corazón, entre otros parámetros. Esta estrategia permite reducir la necesidad de visitas al centro de asistencia primaria. Se informa de este tipo de iniciativas con mayor frecuencia en Europa (OMS, 2011).

En algunos hospitales del mundo se han utilizado sistemas de identificación por radiofrecuencia (RFID, por las siglas en inglés de *Radio Frequency Identification*), que permiten almacenar y recuperar datos remotamente. Una de las modalidades más comunes es la de proveer a los pacientes brazaletes que contienen etiquetas RFID. Estas etiquetas pueden almacenar información adicional y monitorizar otros componentes como identificación del paciente, admisión, transferencia, altas, administración de drogas, localización física del paciente (poten-

cialmente útil en asistencia primaria). Una encuesta realizada al público en general en los Estados Unidos mostró que existía interés en estos dispositivos RFID para monitorizar aspectos de la salud como pulso o presión arterial (Curioso, 2014).

Una de las tendencias más recientes en Europa se relaciona con los sistemas de salud personales, que proveen cuidados personalizados vía dispositivos usables, portátiles o implantables con el objetivo de emitir un diagnóstico temprano o manejar condiciones remotamente (OMS, 2011 y Riva y otros, 2011).

— *Acceso a información:* publicaciones, bases de datos bibliográficos y otros.

Existen ejemplos de servicios que proveen acceso a información, incluidas publicaciones relacionadas con las ciencias de la salud y acceso inmediato a bases de datos mediante dispositivos móviles. Txt2MEDLINE[87] es un método alternativo para la búsqueda en MEDLINE/PubMed mediante consulta por mensaje de texto desde dispositivos móviles. El usuario envía una consulta abreviada por SMS y obtiene mensajes cortos con resúmenes de artículos disponibles en MEDLINE/PubMed. Txt2MEDLINE ha sido probado en países en desarrollo, como Botswana. Este tipo de recursos puede proporcionar un modelo de acceso a información científica a los trabajadores de la salud vía mensajes de texto con información clave a celulares allí donde el acceso a Internet es limitado (Curioso, 2014).

Para maximizar el impacto de la salud móvil y garantizar su continuidad es imprescindible desarrollar aplicaciones y servicios que se integren con los sistemas de historia clínica electrónica. Además de la interoperabilidad, también es muy importante considerar cuidadosamente los diversos aspectos legales, organizativos y tecnológicos relativos a la seguridad y confidencialidad de la información de los usuarios.

---

87 Txt2MEDLINE (2006), *«Txt2MEDLINE: Text-Messaging Access to MEDLINE/PubMed»* [en línea]: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1839569/pdf/AMIA2006_0259.pdf [Consulta:20/06/2015].

6.24 EL SISTEMA DE HISTORIA CLÍNICA DIGITAL DEL SISTEMA NACIONAL DE SALUD ESPAÑOL

6.24.1 CONTEXTO GENERAL

El Proyecto de Historia Clínica Digital en el Sistema Nacional de Salud (SNS) español se define en los primeros meses del año 2006, para responder a las necesidades de los ciudadanos cuando éstos requieren de los profesionales atención sanitaria en situación de movilidad (fuera de la Comunidad Autónoma en la que habitualmente son atendidos). Los Servicios de Salud, en el ámbito territorial de cada Comunidad Autónoma, han venido implantado sistemas automatizados de recogida y gestión de los datos individuales de salud de las personas que dan soporte, entre otros, a los procesos asistenciales, favoreciendo un aumento en los niveles de calidad ofrecida.

Tanto La Ley 16/2003 de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, en su artículo 56, como la Ley 41/2002 de 14 de noviembre, básica reguladora de la autonomía del paciente, en su disposición adicional tercera, dirigen al Ministerio de Sanidad y Consumo el mandato de coordinar los mecanismos de intercambio electrónico de información clínica y salud individual, para permitir el acceso tanto al usuario como a los profesionales en los términos estrictamente necesarios para garantizar la calidad de la asistencia y la confidencialidad e integridad de la información.

Al mismo tiempo, la propia dinámica social, donde la movilidad de los ciudadanos es cada vez más frecuente, hace necesaria la implantación de un sistema que facilite la extensión territorial de dichas funcionalidades al conjunto del SNS y permita a los profesionales la posibilidad de disponer de la información precisa cuando las necesidades de atención sanitaria se producen fuera de la CA en la que se ha generado esta información.

La Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS) tiene como finalidad garantizar a ciudadanos y profesionales sanitarios el acceso a la documentación clínica más relevante para la atención sanitaria de cada paciente. Se incluye documentación que se encuentre disponible en soporte electrónico en cualquier lugar del SNS, asegurando a los ciudadanos que la consulta de sus datos queda restringida a quien esté autorizado para ello.

El proyecto HCDSNS ha sido liderado por el Ministerio de Sanidad, Servicios Sociales e Igualdad en el marco del «Programa Sanidad en Línea» (fases I y II)[88], en colaboración con la Entidad Pública Empresarial «red.es» con las 17 Comunidades Autónomas y con el Instituto Nacional de Gestión Sanitaria (INGESA), encargado de la asistencia sanitaria pública en las Ciudades Autónomas de Ceuta y Melilla (Ministerio de Sanidad, Servicios Sociales e Igualdad, 2009).

6.24.2 OBJETIVOS GENERALES

Los objetivos generales del Proyecto de Historia Clínica Digital en el Sistema Nacional de Salud (HCDSNS) fueron:

— Garantizar al ciudadano el acceso por vía telemática a los datos de salud, propios o de sus representados, que se encuentren disponibles en formato digital en alguno de los Servicios de Salud que se integran en el SNS, siempre que cumplan los mínimos requisitos de seguridad establecidos para proteger sus propios datos contra la intrusión ilegítima de quienes no hayan sido facultados para acceder.

---

88 Sanidad en Línea Fase I: Durante la primera fase del programa Sanidad en Línea, se estableció el marco jurídico para el trabajo conjunto entre el Ministerio de Industria, Energía y Turismo –a través de Red.es–, y el Ministerio de Sanidad, Servicios Sociales e Igualdad con las 17 comunidades autónomas y con el Instituto Nacional de Gestión Sanitaria (INGESA), encargado de la asistencia sanitaria pública en las Ciudades Autónomas de Ceuta y Melilla. Al mismo tiempo, durante esta primera fase, se articuló el modelo de gestión para alcanzar los objetivos propuestos. El Ministerio de Sanidad, Servicios Sociales e Igualdad asumió funciones de coordinación y liderazgo de los proyectos estatales, la ampliación del Nodo Central del Sistema Nacional de Salud (SNS) y el proyecto Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS). La ejecución se llevó cabo en el periodo 2006 -2010 y contó con un presupuesto de 252 millones de euros, de los cuales red.es aportó 140 millones, el Ministerio de Sanidad, Servicios Sociales e Igualdad, un millón de euros y las Comunidades Autónomas, 111 millones de euros. Ministerio de Sanidad, Servicios Sociales e Igualdad (2015): «Sanidad en Línea Fase I» [en línea]: http://www.red.es/redes/actuaciones/sanidad-en-linea/sanidad-en-linea-fase-i [Consulta: 20/03/2015].

— Garantizar a los profesionales sanitarios, facultados por cada Servicio de Salud para esta función y autorizados en cada caso por el paciente, el acceso a determinados conjuntos de datos de salud, generados en una Comunidad Autónoma distinta de aquélla desde la que se requiere la información, siempre que el usuario o paciente demande sus servicios profesionales desde un centro sanitario público del SNS.

— Dotar al SNS de un sistema seguro de acceso que garantice al ciudadano la confidencialidad de los datos de carácter personal relativos a su salud.

— El sistema a desarrollar deberá dotarse de agilidad y sencillez en el acceso, al servicio de ciudadanos y profesionales (Ministerio de Sanidad, Servicios Sociales e Igualdad, 2009).

6.24.3 DISEÑO FUNCIONAL

Funcionalidades para ciudadanos: En este sistema, los ciudadanos tienen la llave de acceso a sus datos y podrán:

— Acceder a los conjuntos de datos personales sobre su salud.

— Ver el Registro de Accesos a sus conjuntos de datos.

— Seleccionar conjuntos de datos que no desea sean accesibles por profesionales de otra Comunidad Autónoma.

Funcionalidades para profesionales: Acceso a los conjuntos de datos personales de un paciente y a sus imágenes

— Para uso exclusivamente asistencial.

— Ante una petición de asistencia del usuario.

Estrategia de seguridad: Se refuerzan las medidas de control previo para el acceso mediante el uso de certificación electrónica que ofrece mayores garantías de autenticidad, la asignación de los profesionales a grupos distintos según la función que desempeñen con acceso a contenidos de información diferenciados según el grupo. Se refuerzan sobre todo los sistemas de control posterior mediante acceso de los propios ciudadanos a los «registros de auditoría interna del sistema», medida en la que juega un papel relevante el propio ciudadano, como auditor externo, al poder llevar a cabo el seguimiento de los accesos realizados a sus datos de salud, o a los de su representado.

Estrategia tecnológica: El Proyecto apuesta por el **principio de neutralidad tecnológica para facilitar la interoperabilidad entre los sistemas de las Comunidades Autónomas**. La estrategia diseñada, partiendo de los sistemas existentes en cada Comunidad Autónoma, **desarrolla una capa de intercambio de información**, facilitando la accesibilidad a la información que se va a compartir. Para ello, se emplea el estándar de mensajería XML como base del intercambio de información entre aplicaciones, y el protocolo de comunicación HTTPS. De esta manera, se independizan las comunicaciones entre sistemas de la plataforma tecnológica utilizada en cada uno de ellos (Ministerio de Sanidad, Servicios Sociales e Igualdad, 2009).

6.24.4 CONTENIDO DE LA HISTORIA CLÍNICA DIGITAL DEL SERVICIO NACIONAL DE SALUD (HCDSNS)

La Historia Clínica Digital del SNS estará formada por todos los conjuntos de datos clínicos que recogen la información relevante para la atención sanitaria que aportan al ciudadano niveles adecuados de calidad en la asistencia al ciudadano fuera de su entorno geográfico habitual.

La Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS) se encuentra conformada por los siguientes documentos de información clínica:

— Informe Clínico de Alta.

— Informe Clínico de Consulta Externa.

— Informe Clínico de Urgencias.

— Informe Clínico de Atención Primaria.

— Informe de Cuidados de Enfermería.

— Informe de Resultados de pruebas de imagen.

— Informe de Resultados de pruebas de laboratorio.

— Informe de Resultados de otras pruebas diagnósticas.

— Historia Clínica Resumida.

Cada uno de estos informes y su contenido recogen de forma resumida los datos que se encuentran recogidos en la Historia de Salud de

cada paciente (Ministerio de Sanidad, Servicios Sociales e Igualdad, 2009).

6.24.5 UTILIDAD PARA PROFESIONALES

Como resultado del análisis de necesidades de los profesionales y ciudadanos, usuarios directos del sistema, se describen 2 grupos de funcionalidades disponibles: 1) para profesionales y 2) para ciudadanos.

El acceso a los conjuntos de datos de salud de un paciente y a sus imágenes queda limitado:

a) Un uso estrictamente asistencial. Sólo cuando el paciente demanda asistencia sanitaria de un profesional fuera de la Comunidad Autónoma en la que reside.

b) Permiso de acceso asociado a grupo, de manera que cada uno de los dos grupos asistenciales definidos en este sistema, médicos y enfermeras, accede sólo a los contenidos necesarios para el desempeño de su función.

Todos los documentos que conforman la HCDSNS, a excepción de la Historia Clínica Resumida (HCR), son documentos que describen episodios concretos y tienen un autor responsable de su contenido. Por ello el formato de presentación es cerrado a fin de que no permita la modificación de sus contenidos originales. El sistema presenta el contenido del informe como imagen para su lectura e impresión, pero no la edición, la copia parcial o total de su contenido, ni su descarga a dispositivos de almacenamiento.

En el caso de la HCR, su generación debe ser automática a partir de la Historia Clínica Electrónica completa y su contenido debe poder consolidarse, total o parcialmente, en la historia clínica electrónica que genera el profesional que realiza la consulta, facilitándole así la incorporación de los datos relevantes. La HCR de la Comunidad de origen seguirá siendo la misma y recogerá sólo las modificaciones que se produzcan en la historia de origen de su propia Comunidad, pudiendo existir tantas HCR de cada paciente como Comunidades Autónomas hayan abierto una historia clínica electrónica (Ministerio de Sanidad, Servicios Sociales e Igualdad, 2009).

6.24.6 UTILIDAD PARA LOS CIUDADANOS

a) *Acceso a los conjuntos de datos personales sobre su salud:* El ciudadano tiene acceso a todos y cada uno de los informes que conforman su HCDSNS, que se encuentran custodiados en cada una de las Comunidades Autónomas en que se han generado.

Todo ciudadano incluido en el registro de usuarios (Base de datos de TSI de su Comunidad) y que se haya dotado de firma electrónica reconocida (o DNI electrónico), podrá acceder a los documentos electrónicos que estén disponibles, a través de la web habilitada por su Servicio de Salud, imprimirlos o descargarlos en un dispositivo de almacenamiento local. Desde el punto de vista jurídico, el derecho de acceso de las personas a sus propios datos de salud fue consolidado por la jurisprudencia y de forma explícita, en la Ley de Autonomía del Paciente que en su artículo 18.1 establece el derecho de acceso a la totalidad de la historia clínica siendo sus dos únicas limitaciones el respeto al derecho a la confidencialidad de terceros y los derechos de los profesionales participantes en su elaboración.

Siendo así, el sistema HCDSNS no hace sino facilitar el acceso por vía electrónica a extractos o partes de la historia clínica, muchos de los cuales ya obran en manos del propio paciente en soporte de papel, sin perjuicio del derecho a la obtención de una copia de su Historia Clínica.

b) *Registro de Accesos producidos a sus conjuntos de datos:* El ciudadano puede realizar el seguimiento de los detalles de los accesos realizados desde este sistema a sus propios conjuntos de datos, a fin de poder verificar la legitimidad de los mismos. Dispondrá para ello de información relativa al momento en que se realizó el acceso, Servicio de Salud, centro sanitario y servicio desde el que se realizó cada acceso, así como las características del documento electrónico accedido.

Cada vez que un ciudadano haga uso de esta funcionalidad ejercerá como auditor externo del sistema, viniendo a sumarse al resto de elementos que conforman la estrategia de seguridad del sistema que, además de los mecanismos implementa-

dos previos al acceso, forma parte de la estrategia de control posterior ya descrita.

Se refuerza con esta funcionalidad el cumplimiento de lo establecido en el Reglamento de desarrollo de la Ley Orgánica 15/1999 de fecha 13 de diciembre, de protección de datos de carácter personal, que en su artículo 96 establece que «a partir del nivel medio (de seguridad) los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente artículo».

c) *Ocultar aquellos conjuntos de datos que no deben ser conocidos por profesionales distintos de quienes habitualmente le atienden:* El reconocimiento de la capacidad del ciudadano de limitar el acceso a parte de sus datos de salud a determinados profesionales ha despertado controversia, por cuanto que no es un derecho explícitamente recogido ni en la legislación española de protección de datos, ni en la legislación sanitaria.

Sin embargo, conviene no olvidar que en la práctica asistencial en el sistema sanitario público y privado español, ésta es una potestad que el ciudadano viene ejerciendo desde siempre. La información plasmada en un informe clínico en papel, facilitada por el propio paciente, sigue siendo el sistema más frecuente por el que el profesional obtiene datos del paciente procedente de un centro distinto de aquel en el que le está atendiendo. La exhibición o no de estos documentos es potestad del paciente. No parece pues pertinente que la implantación de un nuevo sistema automatizado y moderno venga ahora a limitar las capacidades que el sistema sanitario le ha otorgado durante décadas.

El Documento del Grupo de Trabajo del artículo 29 de la Unión Europea sobre Protección de Datos en la Historia Clínica, que no tiene carácter normativo, recomienda, sin embargo, en su apartado III, 3, b, que los sistemas de HCE doten de esta potestad a los ciudadanos. Esta cuestión se puso de manifiesto en los debates de los grupos de trabajo del proyecto HCDSNS, en los que participaron profesionales, gestores, ciudadanos, juristas y bioeticistas. Sin embargo, finalmente acordaron aceptar la inclusión de esta funcionalidad en el diseño del sistema, reconociendo que el paciente, en pleno ejer-

cicio de su autonomía, asume la parte de responsabilidad que le corresponde en los resultados de la atención sanitaria recibida.

Es importante destacar que los datos sobre los que el ciudadano ejerce el derecho de ocultación, en ningún caso son borrados del fichero y la decisión de ocultar puede ser revertida por el propio usuario en cualquier momento.

Al mismo tiempo, sistemas como el de HCDSNS, que hacen uso de los recursos que la tecnología actual ofrece, permiten dejar rastro de las decisiones adoptadas por los diferentes agentes que intervienen en el tratamiento de la información y facilita la auditoría de las mismas.

El sistema HCDSNS contiene además varias salvaguardas disponibles en el ejercicio de esta capacidad, reconocida al paciente:

— En primer lugar, antes de ejecutar la ocultación de un documento, el sistema advierte siempre al ciudadano de las consecuencias negativas que ello puede ocasionarle por condicionar la toma de decisiones del profesional, que debe realizar el proceso diagnóstico y terapéutico sin contar con toda la información existente.

— En segundo lugar, siempre que un profesional de otra Comunidad Autónoma tenga que acceder a la historia del paciente, será informado de la existencia de información oculta (sin la especificación de qué tipo de información se trata) por si, en el contexto clínico concreto, el conocimiento de toda la información fuera de tal trascendencia que, tras informar al paciente, éste entendiera la conveniencia de desproteger los contenidos no visibles.

— En tercer lugar, dado que para el ejercicio de la autonomía es condición necesaria la capacidad del paciente para decidir, ante un juicio de incapacidad, formulado por el profesional en la entrevista clínica, en una situación urgente que requiera actuación indemorable, el sistema le permite acceder a la información inicialmente no visible, pese a la decisión previamente adoptada por el paciente, dejando rastro de la concurrencia de ambas circunstancias, a juicio del profesional (Ministerio de Sanidad, Servicios Sociales e Igualdad, 2009).

6.24.7 PROTECCIÓN DE LA INTIMIDAD DE LAS PERSONAS

Tal como se ha comentado anteriormente, la estrategia de seguridad en este sistema adquiere una relevancia fundamental, puesto que deberá dar respuesta a la protección de datos especialmente sensibles, como son los de salud de las personas, y que requieren para su tratamiento del uso de medidas de seguridad de nivel alto, como establece la Ley de Protección de Datos y el Real Decreto 1720/2007 que aprueba el Reglamento que la desarrolla. Adicionalmente a los requisitos de seguridad impuestos por la legislación vigente, y dado el carácter de la información a manejar, los servicios del Sistema Nacional de Salud dispondrán de mecanismos de seguridad, que mediante el uso de técnicas de criptografía y clave pública garanticen:

— La identidad de las personas previamente autorizadas.

— La autenticidad de los agentes que dicen actuar en su nombre.

— La garantía de no repudio, evitando el no reconocimiento por parte de los agentes de la realización de una operación en el sistema.

— La privacidad de la información objeto del intercambio, de forma que ésta no sea revelada a terceros de ninguna forma, ni intencionada ni accidental.

— La integridad de la información, garantizando que ésta no ha sido manipulada en ningún punto de la comunicación (ni intencionada ni accidentalmente) (Ministerio de Sanidad, Servicios Sociales e Igualdad, 2009).

6.25 INFORME DE CUMPLIMIENTO DE LA LOPD EN HOSPITALES

La Agencia Española de Protección de Datos (AEPD) ha observado últimamente un incremento en las reclamaciones relativas al ejercicio de los derechos de acceso, rectificación, cancelación y oposición en relación con las Historias Clínicas, planteadas por ciudadanos que no han sido atendidos adecuadamente en centros hospitalarios, así como del número de procedimientos tramitados por la Agencia vinculados a la vulneración de los deberes de seguridad y secreto por

parte de centros sanitarios. En particular, en 2009 se registraron un total de 123 denuncias y actuaciones previas de investigación en el sector de la sanidad.

Dada la importancia de estos tratamientos de datos y la trascendencia del derecho fundamental a la protección de datos en este sector, en el mes de marzo de 2010 la Agencia tomó la iniciativa de elaborar el «*Informe de cumplimiento de la LOPD en Hospitales*» y remitirlo a cada uno de los centros públicos y privados que componen el Catálogo Nacional de Hospitales, con el objeto de conocer el nivel de cumplimiento de la LOPD y de su normativa de desarrollo en centros hospitalarios, para adoptar las medidas que resultasen pertinentes.

6.25.1 EL MARCO LEGAL APLICABLE

— La Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su Reglamento de desarrollo, aprobado mediante Real Decreto 1720/2007 de 21 de diciembre (RLOPD), establecen el marco general que regula el derecho fundamental de protección de datos.

— Ley 14/1986, de 25 de abril, General de Sanidad.

— Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

6.25.2 ALCANCE Y METODOLOGÍA

La evaluación del nivel de cumplimiento de la normativa de protección de datos personales se ha realizado mediante el envío a los centros sanitarios incluidos en el Catálogo Nacional de Hospitales que se encuentran bajo la competencia de esta Agencia, consistente en un cuestionario del que se ha requerido su cumplimentación.

La relación de centros hospitalarios objeto del requerimiento se ha obtenido a partir del Catálogo de Hospitales 2009, publicado en el sitio web del Ministerio de Sanidad y Política Social a fecha 1 de marzo de 2010. El Catálogo Nacional de Hospitales es fruto de la colabo-

ración entre el Ministerio de Sanidad y Política Social y las Consejerías de Sanidad de las Comunidades Autónomas, el Ministerio de Defensa, los órganos competentes de las Ciudades Autónomas de Ceuta y Melilla y los propios Hospitales.

El requerimiento fue enviado a los 654 centros que se encuentran en el ámbito de competencia de la Agencia Española de Protección de Datos. Por lo tanto, no han sido objeto de esta actuación los centros de las Comunidades Autónomas de Madrid, Cataluña y del País Vasco, que se encuentran bajo control de las Agencias de Protección de Datos de Madrid, Cataluña y País Vasco, respectivamente.

El colectivo de centros, objeto del estudio, se ha circunscrito a 605 al haber sido eliminados aquellos centros para los que se producían algunas duplicidades en el Catálogo, o bien habían cesado su actividad. Una vez finalizados los plazos de requerimiento se ha recibido la contestación de 562 centros (92,9% del total).

6.25.3 RESULTADOS POR COMUNIDADES AUTÓNOMAS

Con carácter general, se observa un alto nivel de cumplimiento de la normativa de protección de datos en las comunidades autónomas de La Rioja y Murcia. En el resto de comunidades el comportamiento varía según el concepto analizado:

— Los centros hospitalarios de las CCAA de Aragón (66,67%) y Cantabria (75%) son los que presentan un menor porcentaje de inscripción de ficheros de datos personales en el Registro General de Protección de Datos (RGPD). En el resto de comunidades, el promedio de inscripción supera el 87% de centros hospitalarios. Estas mismas comunidades son la que cuentan asimismo con un menor porcentaje de hospitales en los que dicha inscripción se mantiene actualizada: en Aragón es sólo un 41% y en Cantabria un 50%. En ambos parámetros, los indicadores están penalizados por el bajo nivel de cumplimiento en los centros sanitarios de titularidad pública.

— Destaca el bajo nivel de cumplimiento del requisito de publicación de la disposición de creación de ficheros de hospitales de titularidad pública en boletín o diario oficial correspondiente,

en las CCAA de Cantabria (25%), Aragón (50%), Canarias (54,5%) y Asturias (58,3%).

— La inclusión de la cláusula informativa conforme al artículo 5 de la LOPD en los formularios de recogida de datos de los pacientes es particularmente baja en los hospitales públicos de Aragón (5%), Castilla y León (23%), Asturias (25%), Canarias (27%) y Galicia (32%).

— La disponibilidad de procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición supera el 75% de los hospitales en todas las CCAA, a excepción de los centros públicos de las comunidades de Cantabria (50%), Valenciana (62%), Canarias (64%) y Asturias (67%), que se sitúan por debajo de ese umbral.

— La contratación de actividades relacionadas con el tratamiento de datos es mayoritaria en los hospitales de todas las CCAA, a excepción de los centros públicos de Extremadura (50%) y Cantabria (53%) en los cuales esta alternativa de gestión está equilibrada con la gestión 100% interna de los tratamientos de datos.

— Aunque en promedio más del 90% de hospitales cuentan con el documento de seguridad preceptivo según el RLOPD, un 45% de los centros públicos de Canarias y 49% de los de la Comunidad Valenciana no disponen de él.

— En el 55% de los centros públicos de Canarias y en el 45% de los de la Comunidad Valenciana las medidas de seguridad aplicadas a los datos de carácter personal no se corresponden con las de nivel alto según el RLOPD.

— El registro de todos los accesos a la información es particularmente bajo en los hospitales públicos de Extremadura (17,6%), Baleares (27,3%), Aragón (38,9%) y Andalucía (40%).

— Por otra parte, el 55% de los centros públicos de Baleares y Comunidad Valenciana no cuentan con procedimientos para la notificación y gestión de incidencias de seguridad, valor sensiblemente superior al registrado en el conjunto de hospitales de titularidad pública (20%).

— La disponibilidad de dispositivos de almacenamiento de documentos (historias clínicas) que cuenten con mecanismos que

obstaculicen su apertura (p.ej. archivadores con cerradura) es particularmente baja en los centros hospitalarios públicos de Cantabria (25%), Galicia (35,5%) y Comunidad Valenciana (48%).

— El nivel de realización de la auditoría bienal de seguridad en los hospitales públicos es muy dispar según la Comunidad Autónoma de que se trate. Así, es particularmente bajo en las comunidades de Castilla y León (7,7%), Asturias (8,3%), Comunidad Valenciana (10,3%), Aragón (16,7%), Canarias (18%) y Cantabria (25%). Por el contrario, es elevado en La Rioja (100%), Galicia (96,8%), Castilla La Mancha (84,2%), Extremadura (82,3%) y Murcia (80%).

6.25.4 CONCLUSIONES DEL INFORME

El informe de cumplimiento de la normativa de protección de datos ha sido contestado por el 92% de los centros hospitalarios requeridos. En el caso del 8% restante se ha dado traslado al órgano encargado de la función inspectora y sancionadora.

En relación con la muestra de hospitales que han contestado al requerimiento, son de destacar las siguientes conclusiones:

— El cumplimiento de la normativa es alto en el conjunto de centros privados, alcanzándose niveles elevados en la mayoría de conceptos clave analizados: inscripción de ficheros (99%), inclusión de cláusulas informativas en los formularios de recogida de datos (94,5%), disponibilidad de procedimientos para atender el ejercicio de los derechos ARCO (97%) y, en general, en la implantación de medidas de seguridad y su auditoría periódica.

— En promedio, y con excepción de las comunidades de La Rioja y Murcia, el nivel de cumplimiento en los centros públicos es menor que en los centros privados. Las mayores diferencias con éstos se dan en la inclusión de cláusulas informativas en los formularios de recogida de datos (55% frente a 94,5%) y en la realización de la auditoría bienal de seguridad (45% frente a 88%). Además de las señaladas, las áreas de mejora más importantes son la instalación de carteles informativos sobre el

derecho a la protección datos, la revisión periódica del documento de seguridad, el registro de todos los accesos a la información, el archivo de las historias clínicas en dispositivos dotados de mecanismos que obstaculicen su apertura, así como la adopción de medidas para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte. Es importante asimismo destacar que en el caso de los hospitales de titularidad pública, los indicadores varían significativamente según el aspecto y comunidad autónoma de que se trate.

— La mayoría de hospitales (86%) han contratado actividades de tratamiento de datos personales. En la práctica totalidad de estos casos se ha incluido en el contrato de prestación de servicios la cláusula informativa prevista en el artículo 12 de la LOPD. Sin embargo, el porcentaje de centros que en este escenario aplican procedimientos de disociación de los datos de carácter personal es todavía bajo (34%).

— La implantación de *la Historia Clínica Electrónica* alcanza al 55% de los hospitales requeridos, siendo mayor en los centros públicos que en los privados (67% frente a 44%).

6.26 DESVENTAJAS DEL USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN EL TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO SANITARIO

A lo largo de la presente investigación se han visto las ventajas que ofrecen las tecnologías de la información y las comunicaciones (TIC) en el ámbito sanitario, pero se hace necesario conocer la otra cara de la moneda, las desventajas, y citar algunas opiniones vertidas por diferentes autores a continuación:

— Fernández Azuela (2004:236) sostiene que los problemas que se plantean con el uso de las tecnologías de la información en Ciencias de la Salud son de diverso tipo: algunos de ellos están relacionados con la integración de la información, la existencia de terminologías dispares, la falta de establecimiento de estándares; otros con aspectos éticos o legales, como los suscitados por la venta de medicamentos *on line*; y los relativos a la segu-

ridad y protección de datos que, por ejemplo, pueden surgir como consecuencia del despliegue creciente de los servicios en Internet para la transmisión de información médica sensible. Desde luego un aspecto fundamental a considerar es la seguridad de la historia clínica electrónica que, al formar parte de una sistema integrado de información clínica, requiere un plan de seguridad y medidas organizativas que afecten a todos los miembros de la institución y plantea como problema a resolver que las medidas de seguridad no colapsen la disponibilidad de la información ralentizando o impidiendo la adecuada atención sanitaria.

— Hay problemas que limitan la expansión del uso de las tecnologías de la información y los principales son técnicos, como la incompatibilidad entre sistemas; económicos, algunas tecnologías resultan caras de implantar; de confidencialidad y seguridad, cuestiones muy importantes en el ámbito sanitario; de formación a nivel nacional, en España la escasez de recursos humanos es el principal obstáculo para explotar algunas de estas áreas.

— Rodríguez Sendín (2005:4) dice que la historia de salud única y centralizada puede quebrar principios básicos de la bioética, como por ejemplo, el de «beneficencia y no maleficencia» del enfermo (debido a que el mayor riesgo de pérdida de la intimidad acrecienta la probabilidad de daños físicos, económicos, laborales, morales, familiares, sociales, del paciente) o el de autonomía debido a la falta de consentimiento, incluso de conocimiento de los enfermos y desconsideración del derecho de los ciudadanos a tener secretos que son un sostén del libre albedrío. Por otra parte, socava a fondo la relación entre médico y enfermo; pero no sólo del enfermo, sino de su familia y hasta de su descendencia.

— Todos los riesgos anteriores pueden ser gratuitos si no hay razón administrativa, económica, epidemiológica, sanitaria ni mucho menos asistencial que aconseje a concertar la información identificando a las personas. Más aún, la proporción de los datos y circunstancias registrados por el médico en un documento clínico que pueda ser provechosa para otros sectores asistenciales o gestores es muy pequeña. Dicho de otro modo,

una pequeña parte de la información clínica del paciente se justifica que salga del centro en el que se produjo, y sólo cuando se requiera, nunca sistemáticamente.

— Ruiz Téllez (2005) dice que existe un constante deseo de orientar el debate a un solo formato de elección. La historia clínica centralizada puede generar situaciones de no operatividad, si el sistema «se cae, se cae para todos». Entre algunos de los argumentos en defensa de dicho modelo se encuentran los de accesibilidad y continuidad asistencial. El modelo autonómico puede añadir un elemento más de complejidad con la creación de 17 modelos de historia clínica centralizada.

— Dicho modelo generará, sin duda, una vulneración del derecho a la intimidad y confidencialidad de los datos sanitarios; muchos de estos son susceptibles de materializarse en un daño importante para la dignidad personal de los pacientes y usuarios (pensemos en información sanitaria que indique VIH, problemas de drogadicción, entre otros). Además, un agente relevante en la asistencia sanitaria, es el profesional sanitario, y consecuentemente de la elección del modelo centralizado de historia clínica, se lanza un mensaje negativo hacia el profesional sanitario: «Usted no puede preservar la información». Los problemas de confidencialidad y secreto médico tienen su origen en el modelo de elección de la historia clínica electrónica.

— González Médel (2005:3) señala que el binomio prestación sanitaria - historia clínica alumbra y desencadena muchos conflictos diarios, estos con mucha frecuencia se producen por la tensión gestora por parte de los directivos y administradores de los centros y servicios sanitarios. Pone como ejemplo un caso extraído de un foro en el que un responsable de enfermería de un centro de salud es compelido por parte de la dirección de enfermería a entregar los datos con un listado nominal de pacientes con úlceras por presión, ante su petición, la dirección dice «me la das o te ceso». El citado ejemplo le hace apostar por un principio esencial: la historia clínica debe quedar en el centro.

A diario las gerencias son bancos de muchos conflictos, pues anteponen su interés a otros derechos e intereses, los gerentes pueden sa-

car lo que quieran. En este contexto los problemas/sentimientos de los profesionales médicos en la consulta son:

— El modelo de historia clínica genera una percepción de no ausencia del control real del trabajo (asistencia) por derivar todo el esfuerzo gestor en otros intereses, esto desencadena en muchos profesionales el «síndrome del quemado».

— No hay transparencia e información sobre el sistema informático, existe sentimiento de vigilancia.

— Al médico se le relega a ser un agente cuya función es únicamente transmitir datos a la gerencia, sensación de sumisión.

— Además, el médico asume inexorablemente en su fuero interno que la custodia de la historia clínica es competencia suya, por lo que en consecuencia se produce una grave sensación de responsabilidad ante hipotéticas pérdidas de las citadas historias clínicas.

De las conclusiones de la «I Jornada sobre la Confidencialidad y el Secreto Médico», organizada por la Organización Médica Colegial (OMC), Comisión de Libertades e Informática (CLI) y Federación de Asociaciones para la Defensa de la Sanidad Pública (FADSP) (2005) se extrae lo siguiente:

— Las nuevas tecnologías de la información y la comunicación sanitaria deben estar al servicio del ciudadano, ayudar al profesional en la mejora de su práctica y suponer un ahorro de recursos para el sistema. Sin embargo, se han impuesto con autoritarismo y resultan poco eficientes.

— La informatización de las consultas y la historia electrónica de salud constituye un factor de progreso, no obstante, en su utilización deben considerarse los peligros para la confidencialidad de los datos, por su almacenamiento fácil de ocultar, su infinita capacidad de copia y transferencia indetectable y de ínfimo coste, y sus ilimitadas posibilidades de procesamiento y cruce. No puede garantizarse que la protección de los datos médicos centralizados sea infranqueable, teniendo en cuenta que el interés y el valor de tanta información son elevados, basta una única fuga, en un único punto para que los daños sean catastróficos e irreparables. El almacenamiento masivo centralizado de la información clínica es el que mayores riesgos supone para el

secreto y la confidencialidad, comparando con las bases de datos distribuidas. Deben por tanto primarse soluciones tecnológicas pequeñas y repartidas, ya posibles, que eviten tal riesgo.

6.27 EL FUTURO

Fernández Azuela (2004:237) sostiene que el futuro que se plantea dentro de la sanidad gracias a los avances tecnológicos conduce a la automatización de los laboratorios, el uso cada vez más frecuente del chip, la monitorización intensiva y personal, la telecirugía robótica, telemedicina y la formación en red a través de ordenadores y móviles provoca nuevos entornos de trabajo en sanidad. Se espera que la aplicación de las tecnologías de la información en el sector sanitario facilite una mejor cobertura de los servicios, incremente la calidad de los diagnósticos y la salud en general y asegure una buena relación coste-beneficio de los servicios, incluyendo la prestación de servicios para áreas remotas y población dispersa. Hoy en día nadie duda de los beneficios de la aplicación de las tecnologías de la información en el campo sanitario ni de la necesidad y celeridad de su expansión.

En el momento actual se están aplicando las TIC a esquemas clásicos del manejo de información, pero la presentación de los datos apenas se diferencia de su captura. La tarjeta sanitaria puede tener utilidad en el almacenamiento y transporte de información así como en el acceso seguro de la historia clínica electrónica.

La aplicación de las TIC en el ámbito sanitario se puede englobar en diferentes apartados que ya están presentes en la actualidad y que lo estarán más en un futuro próximo:

— *Autocita:* cualquier persona puede acceder a la agenda de su centro de salud para pedir cita en la fecha y en la hora que más le convenga, así se ahorra llamadas telefónicas y esperas en las colas. Los pacientes crónicos pueden enviar por correo electrónico datos que tienen que controlar periódicamente (las mediciones de glucosa de sangre, en el caso de los diabéticos, por ejemplo) para que el personal de enfermería valore su evolución, y si es pertinente, aconsejarle sin necesidad de verle en persona.

— *Historia clínica:* electrónica y única para todos los ámbitos asistenciales, ya sean ambulatorios, centros de especialidades u hospitales. Así será la historia clínica de todos los pacientes, en ella figurarán los datos puramente administrativos, así como las incidencias clínicas de cada individuo. Análisis, resultados de pruebas diagnósticas, imágenes y cualquier información sociodemográfica que sea útil desde el punto de vista asistencial quedará reflejada y clasificada en este documento.

— La historia clínica electrónica se ha favorecido con la incorporación de nuevos dispositivos como los *tablet PC*, tecnologías de reconocimiento de voz y escritura manual, teléfonos móviles inteligentes, brazaletes que contienen etiquetas (RFID) desglosar, entre otros. También Internet se incorporará con mayor importancia a la historia clínica electrónica al facilitar la interacción con todos los ámbitos, en especial el social, influyendo en la recogida y presentación de datos.

— *Receta electrónica*[89]*:* ninguna prescripción se hará ya a mano, pero el reto de la receta electrónica es más ambicioso. El farmacéutico puede participar más en la prescripción de los medicamentos, alertar sobre posibles interacciones, cambiar impresiones con el facultativo y aconsejar mejor al paciente. Este no tiene que guardar papeles ni acudir al centro de salud sólo por recetas, lo que descargará las consultas hasta en un 20% de las visitas de pacientes crónicos.

---

[89] Receta electrónica en el Sistema Nacional de Salud de España: Implantada al 100% en tres (3) Comunidades Autónomas: Andalucía, Baleares y Extremadura. Cinco (5) Comunidades: Canarias, Cataluña, Galicia, la Comunidad Valenciana y el País Vasco están extendiendo el servicio. El resto de Comunidades, han abordado la primera fase del proyecto de receta electrónica. En el SNS español el 42% de las farmacias pueden dispensar medicamentos electrónicamente. La receta electrónica está operativa en el 40% de los centros de salud y disponible para un 26% de la población. En 2009 el 18% de las dispensaciones realizadas en España fueron electrónicas. Plan Avanza 2 (2010), *«Las TIC en el Sistema Nacional de Salud. El Programa Sanidad en Línea»* Ministerio de Sanidad y Política Social y Ministerio de Industria, Turismo y Comercio [en línea]: http://www.msssi.gob.es/profesionales/hcdsns/TICS/TICS_SNS_ACTUALIZACION_ES_2010.pdf [Consulta: 24/06/2015].

— *Red nacional*[90]*:* se trata de un complejo proyecto a largo plazo que exige una titánica labor de coordinación, así como una inversión considerable. Sin embargo, tendrá que llegar el día en el que todos los centros de España puedan trabajar en red. Es decir, se accederá a los datos del paciente independientemente del lugar en el que reciba asistencia. De esta forma, se dispensará una atención mucho más ágil y se solventarán todos los problemas que actualmente plantean los casos de individuos trasladados.

— *Conexión:* la red nacional y acceso generalizado a Internet posibilitarán el intercambio de conocimientos. Los equipos médicos podrán pedir opinión, consultar sus dudas con otros colegas, enviar resultados de pruebas e imágenes para que sean valorados en instituciones de referencia y solicitar recursos que estén disponibles en otros lugares. La formación continuada también será más fácil, ya que los médicos podrán asistir a teleconferencias, cursos, bibliotecas *on line* desde su ordenador.

---

90 Nodo Central de intercambio de información del Sistema Nacional de Salud: La arquitectura de Servicios del Sistema Nacional de Salud es un proyecto tecnológico que se enmarca dentro de la iniciativa europea i2010 y el Plan Avanza para el Desarrollo de la Sociedad de la Información y el Conocimiento. El sistema posibilita el intercambio de información para la Base de Datos de Usuarios de Tarjeta Sanitaria, Fondo de Cohesión, Instrucciones Previas, Registro de Profesionales Sanitarios, receta electrónica, historia clínica y otros servicios. Los servicios del Sistema Nacional de Salud (SNS) se basan en un esquema de interoperabilidad que posibilita la integración de los distintos sistemas de las Comunidades Autónomas al utilizar estándares de intercambio de información a través de mensajes XML y permitiendo la independencia de las plataformas y de las aplicaciones. El Sistema Nacional de Salud se configura tecnológicamente como una arquitectura orientada a servicios (SOA) que apoya la descentralización poniendo a disposición de los Servicios de Salud de las autonomías la información y los servicios que garantizan la atención sanitaria al ciudadano. A través de la Intranet Sanitaria, el intercambiador de XML del SNS es el nexo de unión entre los diferentes agentes (Comunidades Autónomas, otros Ministerios, etc.) que interactúan con los Servicios SNS y viceversa. Plan Avanza 2 (2010), *«Las TIC en el Sistema Nacional de Salud. El Programa Sanidad en Línea»* Ministerio de Sanidad y Política Social y Ministerio de Industria, Turismo y Comercio [en línea]: http://www.msssi.gob.es/profesionales/hcdsns/TICS/TICS_SNS_ACTUALIZACION_ES_2010.pdf [Consulta: 24/06/2015].

— *Urgencias:* las ventajas de la informatización se harán patentes especialmente en urgencias. En un área donde el tiempo es valioso, estos recursos contribuirán a clasificar rápidamente a los ingresados para atenderles en función de su gravedad. Además, al tener todos sus datos clínicos relevantes en el acto (patologías, alergias, etc.), se agiliza la atención y la toma de decisiones, se evitan pruebas innecesarias y se eliminan los errores que a veces pueden derivarse de la necesidad de actuar con tanta premura. Las TIC pueden realizar varias aportaciones que resultan muy valiosas para la práctica clínica. Para ello es necesario que cuenten con las siguientes características en relación al Hardware: 1) autonomía suficiente y tiempo de carga posterior rápido, 2) rapidez y facilidad de manejo, 3) robustez, ligereza y portabilidad, 4) memoria suficiente para un funcionamiento ágil y 5) pantalla con tarjeta gráfica dedicada. En relación al software: 1) acceso a la historia clínica del paciente, 2) atención asistida por ordenador, 3) conexión con apoyos externos, 4) posibilidad de intercambio de información en tiempo real con especialistas hospitalarios, incluida la transmisión de imágenes, 5) localización automática de vehículos, domicilios o lugares de la vía pública mediante dispositivos de localización global (GPS), 6) asistencia en la detección y comunicación precoz de enfermedades trasmisibles graves, 7) compatibilidad. 8) fiabilidad, 9) garantía de privacidad de datos y actuaciones y 10) trazabilidad y auditoría, con posibilidad de explotación estadística de los datos. Finalmente comunicaciones: conexión móvil de tercera generación (3G) (Betelu Corcuera, 2014).

— *Telemedicina:* las zonas rurales o de mayor dispersión demográfica, los operados y los pacientes crónicos serán los principales beneficiarios de la asistencia a distancia. De esta forma, el individuo podrá consultar con sus facultativos pequeñas dudas sin necesidad de desplazarse, al mismo tiempo que el equipo médico podrá supervisar procesos crónicos desde lejos. Un paciente podrá ser dado de alta en menos tiempo, ya que el seguimiento postoperatorio básico podrá hacerse gracias al correo electrónico. La aplicación de la telemedicina es mayoritariamente de carácter clínico (diagnóstico, tratamiento, supervisión y consulta de segunda opinión, entre otros), pudiendo emplearse en casi cualquier disciplina médica, ya sea en tiempo real o

en diferido: radiología, cardiología, encefalografía, neurofisiología, dermatología, patología, oncología, oftalmología, pediatría, psiquiatría, terapia intensiva/UCI, trauma, emergencias, cirugía, rehabilitación, asistencia a domicilio y otros. Sin embargo, la telemedicina puede extenderse también a otros ámbitos como la educación y formación, la investigación, la salud pública o la gestión de servicios de salud. Entre los potenciales beneficios de la telemedicina pueden darse los siguientes: 1) mayor accesibilidad a los servicios sanitarios, 2) incremento de la calidad de las prestaciones de salud, 3) reducción de los tiempos de espera, 4) optimización de los sistemas de atención primaria, 5) mejora de la eficiencia del sistema (Ricur, 2012).

— *Control:* con la instauración de todos estos recursos y la protección de sus datos garantizada (gracias al establecimiento de niveles de acceso, de sistemas de claves y de la firma electrónica), el paciente podrá tomar un papel más activo en el cuidado de su salud, tendrá la posibilidad de programar sus citas y consultar dudas. El médico y el personal de enfermería, harán seguimientos más exhaustivos y, al mismo tiempo, menos asfixiantes ya que las consultas quedarán más despejadas.

6.28 INICIATIVAS DE PROYECTOS CON TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN EL ÁMBITO SANITARIO DE BOLIVIA

6.28.1 SEGURO SOCIAL UNIVERSITARIO

Este seguro fue creado como Seguro delegado de la Caja Nacional de Salud, para otorgar prestaciones de salud a todos los trabajadores docentes y administrativos de la universidad estatal «Mayor de San Andrés».

El Seguro Social Universitario es una institución de servicio y derecho público, con personería jurídica, patrimonio propio, autonomía de gestión técnica, financiera y administrativa y está vinculado a las instituciones más representativas que trabajan en el ámbito de la seguridad social.

El Seguro Social Universitario es miembro del Sistema Integrado de la Seguridad Social Universitaria Boliviana (SISSUB) y de la Organización Iberoamericana de Seguridad Social (OISS), por cuyo intermedio forma parte de los Congresos Iberoamericanos de Seguridad Social y está supeditado al control y fiscalización del Instituto Nacional de Seguros de Salud (INASES). En el transcurso de su actividad, se ha consolidado como un organismo serio y responsable que amerita el respeto y el apoyo de todos los organismos vinculados a la seguridad social en Bolivia y los países iberoamericanos.

La institución tiene como misión fundamental el otorgar prestaciones de salud, tanto en especie como en dinero a favor de toda su población protegida, para su curación y rehabilitación total, con el único fin de velar por el bienestar del capital humano, brindando prestaciones con oportunidad, calidad y calidez buscando en lo posible optimizar los recursos económicos que se tienen y logran la satisfacción del usuario.

El seguro social universitario ofrece las siguientes prestaciones:

— Seguro de enfermedad.

— Seguro de maternidad.

— Seguro de riesgos profesionales a corto plazo.

El Seguro Social Universitario y la Universidad Mayor de San Andrés (UMSA) acordaron poner en vigencia el Seguro Universitario Médico Estudiantil (SUME) para brindar atención médica a estudiantes de ciudad y provincias de la UMSA que estén debidamente inscritos, en forma activa y que no pertenezcan a otros seguros. Aproximadamente 80.000 estudiantes, de las 13 facultades y 54 carreras, de la Universidad Mayor de San Andrés (UMSA) tendrán acceso al Seguro Social Universitario, con una atención integral.

El Seguro Social Universitario de la UMSA cuenta con un moderno hospital de segundo nivel, que tiene todas las especialidades.

Todas las universidades estatales cuentan con el Seguro Social Universitario, a excepción del Departamento de Pando; es decir, que ocho (8) de nueve (9) Departamentos de Bolivia cuentan con el Seguro Social Universitario.

Se desarrolla un software por una empresa nacional para el manejo de la historia clínica por medios electrónicos. En la gestión 2007 ya

se realiza una capacitación a algunas Unidades como Bacteriología, Rayos X, Enfermería, para conocer cómo se lleva a cabo el funcionamiento del mismo.

Todos los consultorios cuentan con una computadora e impresora, los protocolos se realizan en la computadora. La historia clínica no se podrá modificar, el médico tiene la obligación de llenar todos los campos antes de guardar y cerrar la historia clínica. Asimismo, tiene perfiles de acceso por especialidad (SSU La Paz, 2015).

6.28.2 CORPORACIÓN DEL SEGURO MILITAR SOCIAL

La Corporación del Seguro Militar Social (COSSMIL) es una institución pública descentralizada con personería jurídica, patrimonio propio e independiente y autonomía técnica y administrativa, autorizada para actuar en actividades empresariales múltiples.

Tiene como misión proteger la salud de los miembros de las Fuerzas Armadas y su grupo familiar, preservar la continuidad de sus medios de subsistencia, dotarles de vivienda compatible con la dignidad humana y, en general, promover el mejoramiento de su nivel de vida.

La Honorable Junta Superior es el órgano de mayor decisión de COSSMIL encargada de fijar su política institucional; la preside el Ministro de Defensa Nacional y está conformada por el Comandante en Jefe de las Fuerzas Armadas de la Nación, el Inspector General de las Fuerzas Armadas, el Comandante General del Ejército, el Comandante General de la Fuerza Aérea Boliviana, el Comandante General de la Fuerza Naval Boliviana, el Presidente de la Unión de Militares del Servicio Pasivo, el Presidente de la Asociación de Suboficiales y Sargentos del Servicio Pasivo y la señora Presidenta de la Federación de Madres, Viudas y Huérfanos de Militares (COSSMIL, 2014).

Los derechos de los asegurados y beneficiarios son:

— Medicina Preventiva.

— Asistencia Médica General.

— Asistencia Médica Especializada.

— Intervenciones Quirúrgicas.

— Maternidad.

— Servicio Dental.

— Fisioterapia y Rehabilitación.

— Servicios Técnicos Auxiliares de.

— Diagnóstico y Tratamiento.

— Suministro de Medicamentos.

COSSMIL cuenta con veintidós (22) Agencias Regionales distribuidas en toda Bolivia, cada una de las cuales cuenta con un Centro Médico según las necesidades de la región, además de desempeñar funciones administrativas y de enlace con las Gerencias y Direcciones Nacionales.

Por su alto nivel de complejidad y enseñanza, el Hospital Militar Central de La Paz está catalogado en Nivel III, en tanto que en los Hospitales de Cochabamba, Santa Cruz, Trinidad, Tarija, Sucre y Oruro están reconocidos como de Nivel II porque cuentan con medicina interna, ginecología, pediatría, cirugía general y otras especialidades de acuerdo a la demanda, además de laboratorios y farmacia. Los demás distritos, Nivel I, cuentan con medicina general, ginecología, pediatría y algunas especialidades de acuerdo a la demanda.

Independientemente del servicio médico propio de cada regional, en caso necesario se recurre al sistema local de compra de servicios a instituciones médicas con las que se tiene suscritos convenios, o dependiendo de la gravedad, algunos pacientes son evacuados a la ciudad de La Paz para su atención en el Hospital Militar Central. Asimismo, en algunos distritos por la capacidad e importancia de los Centros Médicos COSSMIL se procede a la venta de servicios.

Tabla 9. Establecimientos de salud COSSMIL

Bermejo	Sanandita
Camiri	Santa Cruz
Cobija	Sucre
Cochabamba	Tarija
Chapare	Trinidad
La Paz	Tupiza
Oruro	Uyuni
Potosí	Viacha

Puerto Suárez	Villamontes
Riberalta	Yacuiba
Rurrenabaque	Guayaramerín

Fuente: Elaboración propia.

A partir de la gestión 2002, COSSMIL, a través de su Departamento de Afiliación, ha sustituido el viejo sistema de afiliación con cámaras Polaroid, por uno moderno denominado Sistema de Afiliación (SAFIL). Es la primera fase de implementación del Sistema Integral de Afiliación y Carnetización digital con Arquitectura Cliente/Servidor que ha sido desarrollado por el personal orgánico de la Corporación.

El antiguo sistema de afiliación y carnetización que utilizaba COSSMIL data de 1.º de enero de 1998 y no contaba con un sistema de registro de asegurados en línea, ocasionando que la institución no tenga información actualizada sobre el universo de afiliados, con los perjuicios económicos consecuentes.

Las dos fases restantes para optimizar la afiliación del personal asegurado consiste en la conexión en red con las Regionales del interior (COSSMIL, 2014).

La Dirección de Sistemas de COSSMIL tiene como tarea fundamental atender los requerimientos de información computarizada, diseñando y desarrollando sistemas informáticos que contribuyan a una más eficiente administración.

Busca la consolidación del Sistema Integrado de Gestión Administrativa (SIGA - 1999), apoyo e información a todas las unidades que lo requieran, mantenimiento de equipos de computación, establecimiento de redes informativas a nivel regional y nacional.

La programación y habilitación de un módulo del SIGA para el control adecuado de dosificación de medicamentos que ingresan y salen de la Farmacia del Hospital Militar Central.

En desarrollo la realización de un análisis para contar con el Sistema de Gestión Hospitalaria (SIGEH - 2004) para el Hospital Militar Central destinado a modernizar la atención a los asegurados con el uso de computadoras enlazadas con historias clínicas, imagenología, laboratorios y farmacia.

El Sistema de Gestión Hospitalaria (SIGEH), desarrollado en el año 2004 por una empresa boliviana, incluye software, equipamiento, cableado estructurado. El sistema cuenta con veintiún (21) módulos. EL SIGEH desarrollado por la empresa boliviana tuvo problemas, por lo que el personal de la Dirección de Informática desarrolló el nuevo diseño del proyecto. Asimismo, se están elaborando los nuevos módulos. Se trabaja también en una nueva base de datos que está considerando la información de la anterior.

En el Módulo de Consulta Externa se registra el diagnóstico del paciente, pero se sigue manteniendo la historia clínica en soporte papel. En la aplicación de éste módulo se tuvo problemas con los médicos, quienes no utilizaban el mismo, por lo que se rediseño la interfaz o ventana en colaboración con el usuario, el médico. Se espera implementar el SIGEH en todas las agencias regionales de COSSMIL, empezando con la red troncal, en las ciudades de La Paz, Cochabamba y Santa Cruz; para ello se va a utilizar una Red Privada Virtual - VPN[91]. En cambio con el SIGA ya hay comunicación en la red troncal (COSSMIL, 2014).

6.28.3 CAJA DE SALUD DE LA BANCA PRIVADA

Con más de 17 años de experiencia (desde 1988) y presencia en toda Bolivia (excepto en el Departamento de Pando) se ha convertido en la mejor empresa de asistencia médica y previsional en el país, desarrollando inteligentemente productos y servicios que permiten ver con optimismo el futuro y proyectarse hacia una nueva era, logrando

---

[91] La Red Privada Virtual (RPV), en inglés *Virtual Private Network* (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet. Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación. Wikipedia (2008): *«Red privada virtual»* [en línea]: http://es.wikipedia.org/wiki/Red_privada_virtual [Consulta: 25/12/2014].

mantener su posición de privilegio; ser la institución con el más alto nivel de excelencia en la prestación de servicios médicos en Bolivia.

La Caja de Salud de la Banca Privada es una institución certificada y acreditada prestadora de servicios con alta capacidad y competencia profesional en el campo de la salud, con infraestructura acorde a las necesidades de su población asegurada, modelos de atención enmarcados dentro del perfil epidemiológico propio de cada regional, de óptimo costo-efectividad y pioneros en el campo de la tecnología y la gestión de calidad.

Tiene como misión atender y proteger la salud de sus asegurados y de sus familias, mediante servicios de calidad acorde a sus necesidades. Ofrecen un cuidado de salud integral a trabajadores de empresas aseguradas a la institución, con una cobertura del 100% para los asegurados titulares y sus beneficiarios directos y del 50% para asegurados beneficiarios de 19 a 25 años en los siguientes servicios médicos:

— Asistencia médica general.

— Asistencia médica especializada.

— Hospitalización e intervenciones quirúrgicas.

— Suministro de medicamentos.

— Exámenes auxiliares de diagnóstico.

— Rehabilitación y fisioterapia.

— Servicio dental.

— Servicio oftalmológico.

La Caja de Salud de la Banca Privada está organizada en una oficina central nacional ubicada en la ciudad de La Paz, con la función principal de planificar, normar, evaluar, controlar y supervisar las políticas, estrategias, planes y programas de salud, que deben ejecutarse y gestionarse en las Regionales.

Tiene tres administraciones regionales con sede en las ciudades de La Paz, Cochabamba y Santa Cruz. Cinco agencias regionales ubicadas en las ciudades de Oruro, Potosí, Sucre, Tarija y Trinidad. Responsables zonales en las ciudades intermedias de Puerto Suárez y Montero dependientes de la administración regional de Santa Cruz; y compra de servicios médicos en Bermejo y Yacuiba, bajo tuición y control de la Agencia Regional de Tarija.

En las ciudades de Beni y Pando, se tiene firmado un convenio interinstitucional con la Caja de Salud de Caminos para la atención médica de sus asegurados.

A diciembre de 2014, la población asegurada de la CSBP, asciende a 87.693 asegurados, entre titulares y beneficiarios, presentándose un crecimiento de 6.1% respecto a la gestión 2013. Cuantitativamente la población de la CSBP crece en 5.012 asegurados, sin embargo, porcentualmente, presenta un decrecimiento del 5.1%. Esta tasa de crecimiento es la más baja que se da en los últimos diez años.

Se debe mencionar que entre la población afiliada, no se toma en cuenta a los 2.160 niños beneficiarios del Proyecto del Seguro Gratuito de Enfermedad y Maternidad de la Ciudad de El Alto, dirigido a la atención médica de niños en extrema pobreza.

6.28.3.1 Software Médico y Sistema Administrativo Médico (SAMI)

El costo del Software 9000 fue de 150.000 dólares americanos, fue adquirido el año 2002 de una empresa peruana de desarrollo especializada en el área de salud. De 2002 a 2004 se trabajó en forma remota con la empresa peruana, básicamente se trataba de un contrato de *outsourcing*[92]; con el transcurso del tiempo, resultó oneroso para la CSBP por la capacitación, mantenimiento, desarrollo de nuevos productos, implementación, validación; aproximadamente unos 40.000 dólares americanos por año.

---

[92] Contrato de *outsourcing* (externalización): La palabra inglesa «*outsourcing*» significa «suministrar externamente». En España este término es traducido como «*externalización*» y en algunos países latinoamericanos como «*subcontratación*» o «*tercerización*» de procesos que significa suministrar a través de terceros. Una definición del Instituto de Estudios Superiores de la Empresa (IESE) señala que el *outsourcing* es: «*La incorporación a la empresa de aquellas competencias que no ha escogido como centrales o nucleares mediante la colaboración con otra empresa. Así, el outsourcing puede aplicarse a todo proceso o función de negocio que no sea estratégico para una empresa y que, consecuentemente, no debe ocupar tiempo de gestión por parte de la dirección*». Instituto de Estudios Superiores de la Empresa IESE-International Research Center on Organizations IRCO (2002). «*Outsourcing de Recursos Humanos*».

En la gestión 2005 la CSBP asume el desarrollo del prototipo funcional, en base a la experiencia del Software 9000 comprado a la empresa peruana. Este nuevo prototipo está hecho a la medida de las necesidades particulares de la CSBP, para ello se realizaron pruebas Alfa para validar la información y el producto final, posteriormente las pruebas Beta, la entrega del producto en funcionamiento del cien por cien, con la información de los asegurados.

La Caja de Salud de la Banca Privada, dentro de su Política de Gestión y Administración Tecnológica, continuamente trabaja en mejorar y actualizar su Software Médico y Sistema Administrativo Médico (SAMI) desarrollado por profesionales de la CSBP, el cual se aplica y utiliza actualmente en los Servicios de Consulta Externa (Policonsultorio) y Hospitalización a nivel nacional.

Esta importante herramienta informática registra, almacena y clasifica toda la información clínica y administrativa de cada paciente. Consiste en una «Historia Clínica Electrónica» con toda la gama de funciones y aplicaciones, contiene la información completa del Expediente Clínico de cada paciente, de forma cronológica, con fecha y hora de atención.

Para el acceso al sistema se cuenta con algoritmos de encriptación y alta seguridad que son como «candados» para que los datos de los pacientes no puedan ser modificados y revelados a terceros, con un sistema de contraseñas de ingreso para cada profesional. De esta manera, se asegura la seguridad y privacidad de la información de cada paciente, garantizando la confiabilidad y confidencialidad de datos clínicos de pacientes, administrativos y reportes por medio de un sistema configurable de usuarios y contraseñas con distintos niveles de acceso.

El Software Médico de la CSBP tiene la particularidad y funcionalidad de contar con una «Historia Clínica Única», lo que significa que cuando el paciente se atiende en otra Regional, que no es la de origen, el médico puede obtener sus datos, información e Historia Clínica y revisar todo su historial médico; además este sistema permite manejar la información en tiempo real a nivel nacional.

Asimismo, el SAMI cuenta con un «Sistema de Alertas» para identificar algunas enfermedades crónicas, como la hipertensión, diabetes, dislipidemia, obesidad y tumores malignos (cuello uterino, próstata, mamas y otros). Mediante este sistema se avisa y alerta al médico

correspondiente el estado de salud y diagnóstico del paciente que está atendiendo en ese momento, con el fin de dar continuidad al tratamiento, emitir una interconsulta médica o simplemente recordarle que acuda a sus controles. De la misma forma, el Sistema SAMI cuenta con diversas fórmulas, entre ellas la de detección precoz de patología renal en niños y adultos, fórmula para el cálculo del Índice de Masa Corporal (IMC) para prevenir y/o controlar el sobrepeso u obesidad, fórmula del ANTRHO desglosar para medir los niveles nutricionales de la niñez (permitiendo el cálculo antropométrico y la evaluación del estado nutricional de los niños en edad escolar y adolescentes), entre otros cálculos.

El Sistema SAMI está constituido por veintiún (21) módulos médico-administrativos, que interactúan entre sí e incluyen las áreas de Afiliaciones, Citas Médicas, Consulta Externa, Hospitalización, Emergencias, Quirófano, Farmacia, Laboratorio, Gabinetes, Tratamientos (Fisioterapia, Enfermería, Psicología, Psicopedagogía, Fonoaudiología, Nutrición, Trabajo Social), servicios externos, facturación, estadística, cotizaciones, sistemas y actividades médicas complementarias. Este sistema médico integra de manera sencilla las áreas de agendas médicas y el expediente clínico electrónico.

La Historia Clínica Electrónica del SAMI permite captar toda la información del paciente, además de clasificarlo de acuerdo al Régimen de Seguro y Programa de Salud, otorgarle órdenes de laboratorio, exámenes auxiliares, prescripciones médicas, órdenes de interconsulta, bajas médicas, certificado prenatal, entre muchos otros documentos. Además, puede obtener informes médicos, informes de junta médica, reportes de estudios comparativos entre la gama de variables con que cuenta el SAMI y reportes de seguimiento a la calidad del registro de la información.

Con esta valiosa herramienta informática se puede realizar una variedad de análisis estadísticos, investigaciones médicas, detección de factores de riesgo más frecuentes en la población asegurada, patologías prevalentes y todo tipo de reportes que sirven para elaborar planes de promoción y prevención, en la perspectiva de que un Sistema de Salud es más eficaz en la medida en que prevenga la aparición de enfermedades más que tenga un enfoque curativo y asistencialista.

SAMI permite integrar de manera completa todas las áreas de Policonsultorio y Hospitalización; con este sinfín de usos y utilidades se

mejora la calidad de la información de las Historias Clínicas y todo ello contribuye a una mejor atención al asegurado, evitando la repetición manual de datos burocráticos en la otorgación de documentos como las bajas médicas, interconsultas, recetas, solicitud de exámenes complementarios y otros.

En el transcurso de la gestión 2014, el Software Médico se ha ido mejorando, complementando y actualizando de acuerdo a las necesidades institucionales, principalmente enfocadas a la puesta en marcha de la nueva Clínica Regional La Paz, acompañando con capacitaciones y actualizaciones continuas en su manejo a los usuarios del sistema.

Es así que el Software Médico de la CSBP proporciona los recursos, dispositivos y métodos necesarios para optimizar la adquisición, almacenamiento, recuperación y utilización de la información en salud, convirtiéndose en una herramienta primordial que va en beneficio del paciente para mejorar la calidad de la atención a nuestra población asegurada.

Siendo el Software Médico SAMI CSBP, la herramienta más importante para el registro de la atención médica, se vio la necesidad de ampliar el Software Médico a la Atención hospitalaria. En este sentido, en la gestión 2014 se dio inicio al Proyecto de Restructuración del SAMI de Hospitalización, con cuatro (4) etapas de desarrollo:

— *Primera Etapa:* Diagnóstico situacional de los módulos, relevamiento de formularios manuales y necesidades de registros de Regional La Paz y Regional Santa Cruz.

— *Segunda Etapa:* Reuniones de coordinación y realización de 54 Talleres por Servicios con equipos de trabajo multidisciplinarios. Se revisaron las unidades hospitalarias y todos los módulos del SAMI que interactúan en Hospitalización y los procesos hospitalarios existentes, además de identificar y elaborar nuevos procesos. En la Regional Santa Cruz, se realizó la validación del SAMI Hospitalario.

— *Tercera Etapa:* Revisión y validación de los módulos del SAMI de Hospitalización (UTI, UTIN, Sala de Partos, Emergencias, Internación, Quirófano, Recuperación, Enfermería, Nutrición, Trabajo Social, Psicología, Fisioterapia, Farmacia).

— *Cuarta Etapa:* Capacitación a usuarios del SAMI Hospitalario e implementación del SAMI de Hospitalización a nivel nacional, seguida de una fase de ajustes a la nueva versión.

La historia clínica electrónica en la CSBP se implementa en forma vertical; es decir, de arriba abajo, se realizan planes de capacitación. Los médicos se capacitan primero, pero es el que dedica menos tiempo a la capacitación por su trabajo, al inicio hay quejas por parte del paciente porque el médico está más preocupado en llenar la historia clínica que en el paciente; así muchas veces al lado del médico está el profesional informático para absolver las preguntas del médico en el manejo del software. Posteriormente, se capacita a las enfermeras; no hubo mayores problemas con este personal, porque son los soldados de la institución. Finalmente, se capacita al personal administrativo (Farmacia, Contabilidad y Estadística).

La implementación de la historia clínica electrónica ha sido positiva para la CSBP, obliga al médico a llenar todas las casillas que requiere información antes de cerrar la historia clínica. En la historia clínica en soporte papel se presentan problemas como: estar sin firma, sin sello, mal llenadas, no se entiende la letra del médico, entre otros. Con la historia clínica electrónica se tiene toda la información de la población asegurada (Nombre, Carné de Identidad, Entidad, Vigencia de Derechos a nivel nacional y la historia clínica del paciente).

La CSBP cuenta con las historias clínicas electrónicas de ocho (8) departamentos de Bolivia, a excepción de Pando (Caja de Salud de la Banca Privada, 2014).

6.28.3.2 **Cita por internet**

Durante la gestión 2013, la Unidad de Atención al Asegurado en coordinación con la Gerencia General encaró el Proyecto de Reserva, Programación y Distribución de Citas Médicas (fichas) a través del Portal Web de la CSBP, inicialmente para las Regionales de La Paz y Santa Cruz.

El mencionado Proyecto se desarrolló con el objeto de mejorar y facilitar el acceso y oportunidad de la atención médica, fortaleciendo el Sistema o Módulo de Programación y Distribución de Citas Médicas (fichas) a través de Internet. Es así que a partir de segundo semestre de la gestión 2013, todos los Asegurados Titulares con Vigencia,

tanto del Sector Activo como del Sector Pasivo (Jubilados o Rentistas), programan y obtienen sus Citas Médicas (fichas) para la atención en el Servicio de Consulta Externa a través del Portal Web de la CSBP (www.csbp.com.bo).

Figura 20. Vista de citas por internet

Fuente: Caja de Salud de la Banca Privada - Software SAMI.

Asimismo, los Asegurados Beneficiarios con vigencia podían contar con una Cita Médica mediante el Sistema o Módulo de Programación y Distribución de Citas Web, por medio del acceso (usuario y contraseña) de su asegurado titular.

Las Citas Médicas (fichas) programadas y distribuidas a través del Portal Web, fueron habilitadas y puestas a disposición de los asegurados con un día de anticipación en el horario de: 17:00 a 20:00 Hrs.

A diciembre de 2013, el 65% de los Asegurados Titulares ya se encontraba registrado en el Módulo de Citas Web, mostrando un comportamiento creciente en el uso del mencionado Módulo para reservar y acceder a la atención médica en el Servicio de Consulta Externa (Caja de Salud de la Banca Privada, 2014).

6.28.3.3 Software de educación virtual *e-learning*

La Caja de Salud de la Banca Privada, como entidad pionera en el uso de tecnología informática, durante la gestión 2014 dio continui-

dad al Software de Educación Virtual (SEV), con el objeto de capacitar y actualizar virtualmente a sus funcionarios en los ámbitos: médico, administrativo y otras áreas de conocimiento.

Este sistema de aprendizaje, a través de la utilización de medios electrónicos se basa en la aplicación de las tecnologías de la información y el conocimiento (TIC), para desarrollar procesos de educación y capacitación a través de Internet. La enseñanza *online* permite el proceso de aprendizaje mediante la utilización de diversas herramientas informáticas orientadas a la asimilación y comprensión de los contenidos de los cursos de capacitación.

La Plataforma Académica Virtual del Software de Educación Virtual (SEV) cuenta con un Programa de Capacitación diseñado de acuerdo al diagnóstico de necesidades de capacitación a nivel nacional.

Durante la gestión 2014 se dio continuidad a los siguientes cursos:

— Curso de Manejo del Software de Educación Virtual para Facilitadores, impartido a todos los facilitadores designados.

— Curso de Manejo del Software de Educación Virtual para Alumnos, impartido a todos los alumnos inscritos a los cursos.

— Curso Teórico Práctico de Dactilografía Médica, impartido a todos los médicos de Administraciones y Agencias Regionales con prácticas en el *Typing Master*.

— Curso de Bioseguridad y Manejo de Residuos en Establecimientos de Salud, impartido a los Comités de Bioseguridad de Administraciones y Agencias Regionales.

— Curso de SQL Server 2000, impartido al personal de Telemática Regional de Administraciones y Agencias Regionales, y personal que maneja bases de datos (Caja de Salud de la Banca Privada, 2014).

6.28.3.4 **Atención asegurado**

Por otra parte y en el marco de la gestión y atención de quejas y reclamos, en la siguiente tabla se puede apreciar los datos e informa-

ción de la gestión y atención de solicitudes, sugerencias y reclamos presentados a nivel nacional durante la gestión 2013.

Tabla 10. Reclamos Registrados Según Área y Tipo de Reclamo Gestión 2014

Área	Reclamos identificados		Reclamos anónimos		Total reclamos	
Cantidad	Porcentaje	Cantidad	Porcentaje	Cantidad	Porcentaje	
Médica	143	77,72%	93	85,32%	236	80,55%
Administrativa	41	22,28%	16	14,68%	57	19,45%
Total Reclamos Recibidos	**184**	**100,00%**	**109**	**100,00%**	**293**	**100,00%**

Fuente de elaboración: Caja de salud de la Banca Privada.

Como se puede observar, el 80.55% de los reclamos presentados por los asegurados y afiliados a la CSBP corresponde al área médica o de salud. Dentro de este segmento se encuentran las observaciones realizadas en la atención por los servicios de enfermería, laboratorio, rayos X y otros servicios auxiliares de diagnóstico, así como también por el acto médico en sí. Asimismo, el siguiente gráfico muestra los motivos de reclamos más recurrentes o frecuentes presentados durante la gestión 2014, los cuales fueron referidos principalmente a la atención médica, diagnóstico y tratamiento, actitud y trato del personal, impuntualidad e incumplimiento de horarios, a accesibilidad y oportunidad de la atención y a la insuficiente información y comunicación.

Una vez que la Unidad de Atención al Asegurado gestiona y atiende los mencionados reclamos, dando una respuesta a los mismos, toda esta información es proporcionada a las diversas unidades de Gestión de Calidad de las Regionales con el objeto de que se planifiquen y ejecuten acciones de mejora continua dentro de lo establecido en el Sistema de Gestión de Calidad de la CSBP (Caja de Salud de la Banca Privada, 2014).

6.28.3.5 Medición de la satisfacción del asegurado

En cumplimiento al Plan Estratégico Institucional (PEI), la Unidad de Atención al Asegurado en coordinación con las Unidades de Tra-

bajo Social, Estadística y Planificación Institucional, y bajo la supervisión de la Gerencia General de la CSBP, gestionaron y encargaron a la Empresa Consultora «CIES Internacional» el desarrollo del estudio e investigación del grado de satisfacción y percepción de los asegurados, tanto titulares como beneficiarios, con los servicios y la atención que se les brinda en la institución, cuyo objetivo es medir y conocer la satisfacción de los asegurados de la CSBP, permitiendo el diseño de estrategias que mejoren el servicio e incrementen la satisfacción de los asegurados; primer objetivo estratégico establecido en el Plan Institucional.

Los resultados de este estudio establecieron que el Índice de Satisfacción de los Asegurados de la CBSP es del 79%, lo que significa que de cada 100 afiliados, 79 están satisfechos. Este índice ha descendido en relación al estudio realizado en la gestión 2012 en 5% (84%), por lo que se encuentra por debajo del promedio o nivel mínimo aceptable establecido por la CSBP determinado en un 80%.

Las Regionales que registran un Índice de Satisfacción de los Asegurados general mayor a la media nacional son Santa Cruz (90%), Cochabamba (82%), Sucre (86%) y Trinidad (85%); mientras que las Regionales que registran un Índice de Satisfacción menor a la media nacional son La Paz (72%), Tarija (76%), Potosí (69%) y Oruro (63%). El desarrollo del mencionado estudio permitirá a la CSBP delinear acciones y estrategias a corto, mediano y largo plazo y tomar decisiones para la mejora continua, con el objeto de incrementar la satisfacción de los asegurados (Caja de Salud de la Banca Privada, 2014).

6.28.4 HOSPITAL ARCO IRIS

En 1997 nacen, en la Fundación Arco Iris[93], los primeros planes para construir una clínica como resultado de una búsqueda de un

---

[93] Fundación Arco Iris: es una organización no gubernamental, basada en los principios de la Iglesia Católica que desde 1994 lucha contra la discriminación, marginación y falta de oportunidades que sufren miles de niños, niñas y jóvenes: huérfanos, cuyos padres están en la cárcel, víctimas de violencia intrafamiliar, maltratos, violaciones, los que viven o trabajan en las calles de la ciudad de La Paz – Bolivia. Para cumplir su objetivo ejecuta numerosos

sistema que atienda las necesidades de salud para Niños de la Calle (NDLC). El primer proyecto de salud estuvo ubicado en un colegio de la zona central de La Paz, donde se trataba ambulatoriamente las dolencias de los que viven en las calles.

En la ciudad de La Paz se tiene alrededor de 30.000 niños que sobreviven como lustrabotas, dulceros, recogedores de basura, voceadores y algunas muchachas como prostitutas. Unos 2.000 viven en las calles sin ningún vínculo familiar, y son víctimas de drogas, alcohol, maltrato y enfermedades infecciosas. Normalmente los niños de la calle no velan por su salud y, por falta de recursos económicos, no tienen posibilidad de acudir a un centro médico.

En agosto de 1998, la *Papstiiches Missionswerk fur Zinder* (PMK – Obra Misionera Papal para los Niños) de Alemania realizó una solicitud de ayuda a la Unión Europea (UE) para un proyecto de cinco (5) años. Gracias a esta ayuda, la Fundación Arco Iris planificó la construcción de un moderno hospital de Segundo Nivel, ubicado en la ciudad de La Paz, la construcción del Hospital Arco Iris se terminó en septiembre de 2001, la inauguración del hospital fue el 27 de septiembre y la apertura el 23 de octubre de 2001.

Las finalidades perseguidas con el hospital fueron: formación, prevención e instrucción sanitaria y rehabilitación, para el grupo meta compuesto por un estimado de 5.000 niños que viven en la calle y otros 30.000 niños aproximadamente que trabajan en la calle. El proyecto debería alcanzar prioritariamente la previsión sanitaria.

El hospital de 100 camas muestra un alto estándar en su infraestructura y equipamiento médico y es considerado como uno de los mejores hospitales en La Paz, donde trabajan cerca de 300 personas. Cuenta con 26 especialidades y atiende cerca de 80.000 personas por año, de las cuales cerca de 4.000 pertenecen a la población principal,

---

proyectos de apoyo integral y realiza campañas de sensibilización entre las personas con espíritu de solidaridad y desprendimiento. Casi en su totalidad, la Fundación se sostiene del apoyo de personas individuales, sin grandes financiamientos de la cooperación internacional o gubernamental. Busca ser un signo de amistad, solidaridad y desprendimiento, en favor de los más pobres, necesitados y desprotegidos. Fundación Arco Iris (2015): «*Hospital Arco Iris*» [en línea]: http://www.arcoirisbolivia.org/mision.html [Consulta: 01/10/2014].

niños de la calle. Tres (3) consultorios móviles además proveen de salud primaria a los niños pobres y principalmente uno de ellos se introduce en las calles donde viven los más desprotegidos y son la meta de la Fundación Arco Iris.

Estos consultorios atienden, por año, cerca de 40.000 niños menores de 18 años, lo cual incluye la provisión de medicamentos en forma gratuita (Fundación Arco Iris, 2015).

A partir de la gestión 2008 se implementa en el Hospital Arco Iris el Sistema Integrado de Administración Financiera (SIAF) y el Sistema de Información Clínico Estadístico (SICE), ambos desarrollados por la Organización No Gubernamental Medicus Mundi y reconocidos por el Ministerio de Salud y Deportes a través de la Resolución Ministerial 0853 de fecha 18 de noviembre de 2005.

Dos profesionales informáticos y un consultor externo realizan el desarrollo de software conforme las necesidades del Hospital. Asimismo, realizan la implementación del SIAF y el SICE.

Se han incorporado al SICE información de servicios de diagnóstico como: Laboratorio, Microbiología, Rayos X, Tomografía y Ecografía. Con la información de las historias clínicas se conforma una base de datos para el SICE.

Existen perfiles de acceso para la utilización del SICE. El procedimiento para recabar una historia clínica consiste en retirar una ficha del sistema, se imprime la ficha y se entrega a la Unidad de Archivo, la cual busca la historia clínica en soporte papel del paciente y la lleva a la Unidad de Enfermería, quien reparte las diferentes historias clínicas a los consultorios médicos. El registro del ingreso y egreso de la historia clínica es manual.

La Unidad de Admisiones puede modificar la historia clínica porque tiene la historia clínica en soporte papel. Los responsables de Área pueden modificar la información del módulo correspondiente. Los Jefes Médicos tienen acceso a la información de los sistemas para conocer el rendimiento del servicio.

El Hospital Arco Iris considera una experiencia positiva la implementación del SIAF y el SICE porque se tiene mayor información clínica, estadísticas en cirugía, entre otra información que sirve para conocer cómo está el funcionamiento del Hospital Arco Iris.

Se tienen estrategias para llegar a los niños de la calle a través ambulancias móviles que van a toda la ciudad mediante un cronograma planificado. Sin embargo, la necesidad de poder sustentar este servicio a los más necesitados impulsó a que se abra la atención de consulta externa a toda la población mediante el uso de una atención privada que genera recursos económicos.

A pesar de ser un Hospital privado, por convenio con Ministerio de Salud, asume atenciones públicas como ser: el Sistema Integral de Salud (SIS) que atiende gratuitamente a niños menores de cinco (5) años y a mujeres gestantes en etapa prenatal, durante el parto y el seguimiento posparto hasta los seis (6) meses. El Estado, a través del Ministerio de Salud, realiza el reembolso de los gastos generados por esta atención conforme a los mismos costos que los hospitales públicos.

Todos los esfuerzos para otorgar una mejor atención a los pacientes se traducen en la incorporación de tecnologías de información y comunicación (TIC) dentro del sistema que maneja el Hospital como un acto más humano en favor de los más necesitados.

Existen dieciséis (16) consultorios con treinta y cinco (35) especialidades mediante los cuales se atiende aproximadamente de trescientos (300) a cuatrocientos (400) pacientes por día. (Fundación Arco Iris, 2015).

CAPÍTULO VII
LA SEGURIDAD DE LA INFORMACIÓN CLAVE PARA EL TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO SANITARIO

7.1 LA SEGURIDAD

«Ser lo que soy, no es nada sin la seguridad», una frase acuñada por W. Shakespeare en el siglo XVI muestra como el hombre tiene la necesidad de vivir en seguridad. Considerando que la adopción de diversos Sistemas de Información es masiva en casi cualquier contexto, surge la necesidad de proteger la información que forma parte de dichos sistemas, pues dicha información se torna crítica e invaluable, pues concentra el día a día de la organización. La «Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y de las posesiones, es tan antigua como ella» (Manunta, 2003).

Si se observa lo que define la Real Academia Española (RAE) como *seguro*, se tienen características importantes como la de estar libre y exento de peligro, daño o riesgo. Toda vez que el activo que se está resguardando se encuentra en los sistemas de información, se puede seguir la definición de Aguilera López (2010:9) que señala que la seguridad de la información «es una disciplina que se ocupa de diseñar normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable». Por lo que se puede entender, respecto a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e integridad de la misma.

De la misma manera, Sanz y Hualde (2000:74) definen a la seguridad como «la característica de un sistema que lo hace ser capaz de proteger sus datos frente a la destrucción, interceptación o modificación no deseadas». Se entiende que la seguridad debe ser una característica de los sistemas de información que almacenan datos de carác-

ter sensible, por lo que se hace muy necesario tenerlo en cuenta en todo el ciclo de desarrollo de los Sistemas de Información.

Si se mira la norma (UNE) ISO/IEC 17799, predecesora de la actual UNE-ISO/IEC 27001, esta recuerda que la información es un activo que hay que proteger, y que puede estar en diferentes tipos de soportes. La norma citada sigue manteniendo tres principios clásicos de la seguridad (conocida como la Triada CIA por sus siglas en inglés):

— *Confidencialidad:* el acceso a la información debe ser restringido en función de la persona que intenta acceder y de la pertinencia de dicho acceso. En otras palabras, se debe establecer quién accede a qué datos, cuándo y cómo.

— *Integridad:* la información registrada debe ser veraz y completa, y para ello debe estar protegida contra accidentes y ataques. Si los datos no son fiables o están incompletos, no son de utilidad.

— *Disponibilidad:* la información debe estar disponible en el momento y lugar en que sea necesaria, independientemente del momento y lugar en el que se haya generado (Blanco y Rojas, 2012).

Se entiende que la disponibilidad estaría dentro de un marco de tiempo variable según el sector y tipo de aplicación y que una situación de no disponibilidad temporal es un riesgo, generalmente mucho menor que la no disponibilidad definitiva por pérdida irreversible de la información correspondiente.

Tabla 11. Necesidades de seguridad

Necesidad	Medidas
Confidencialidad	Definición de permisos: determinar quién *puede* acceder al sistema y a qué información *puede* acceder.
	Control de accesos: conocer quién accede realmente al sistema y a qué información accede.
	Protección del sistema: *impedir* accesos no autorizados.
Integridad	Protección de la información: evitar la *alteración* o *pérdida* de datos, y garantizar su *recuperación* en caso necesario.
	No repudio: impedir que un agente implicado en el tratamiento de la información niegue su participación.

Necesidad	Medidas
Disponibilidad	Definición de los niveles de servicio correspondientes.
	Adaptación de los sistemas de información a los niveles de servicio.
	Dotación de los recursos necesarios para garantizar el nivel de servicio.

Fuente: Rojas y Blanco, 2008.

El Instituto Nacional de Tecnologías de la Comunicación de España (INTECO) señala que existen numerosos e importantes beneficios para implementar Sistemas de Seguridad de la información, como por ejemplo:

— *Reducción de costes:* Incide directamente sobre la rentabilidad económica de una organización. No suele serlo porque lo que se ve en un principio es el coste del mismo; sin embargo, en un breve plazo, se puede observar como los diferentes mecanismos de seguridad de la información evitan varias situaciones que suponen un coste, a veces importante.

— *Optimizar los recursos y las inversiones en tecnología:* Con medidas de seguridad de la información correcta, las decisiones se tomarán en base a información fiable sobre el estado de los sistemas de información y a los objetivos de la organización. La organización dejará de depender exclusivamente de la experiencia o pericia del responsable de informática, o más peligroso aún, del proveedor habitual de informática a la hora de valorar las distintas opciones de compra.

— *Protección del negocio:* La Seguridad de la información en marcha evita interrupciones en el flujo de ingresos, ya que se está asegurando de una manera eficaz la disponibilidad de los activos de información y, por lo tanto, de los servicios que la organización ofrece. Esto en cuanto a la actividad cotidiana; pero también se está preparado para recuperarse ante incidentes más o menos graves e incluso garantizar la continuidad del negocio, afrontando un desastre sin que peligre el negocio a largo plazo.

— *Mejora de la competitividad:* Cualquier mejora en la gestión de la organización tiene consecuencias directas en beneficio de la eficacia y la eficiencia de la misma, haciéndola más competiti-

va. Además hay que considerar el impacto que suponen el aumento de la confianza de los clientes en el negocio, la diferenciación frente a los competidores y una mejor preparación para asumir retos tecnológicos.

— *Cumplimiento legal y reglamentario:* Cada vez son más numerosas las leyes, reglamentos y normativas que tienen implicaciones en la seguridad de la información. Gestionando de manera coordinada, la seguridad permite un marco donde incorporar los nuevos requisitos y poder demostrar ante los organismos correspondientes el cumplimiento de los mismos.

— *Mantener y mejorar la imagen corporativa:* Los clientes percibirán la organización como una empresa responsable, comprometida con la mejora de sus procesos, productos y servicios. Debido a la exposición de cualquier organización a un fallo de seguridad que pueda acabar en la prensa, este punto puede ser un catalizador de esfuerzos, ya que nadie quiere que su marca quede asociada a un problema de seguridad o una multa por incumplimiento, por las repercusiones que acarrea (INTECO, 2010).

La Sociedad Española de Informática de la Salud (SEIS) señala que existen varios aspectos relevantes respecto a la seguridad, tal como se muestra en la figura siguiente:

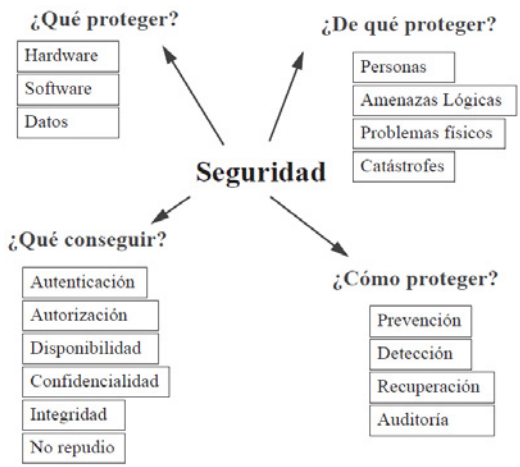

Figura 21. Elementos de la seguridad

Fuente: La Seguridad y Confidencialidad de la Información Clínica (SEIS).

En este sentido, se analizarán estos elementos necesarios para procurar la seguridad necesaria de los Sistemas de Información en el entorno sanitario.

7.2 ¿QUÉ PROTEGER?

Todo sistema informático contiene tres (3) elementos que deben ser protegidos; estos son el hardware, el software y los datos.

Al estar frente a Sistemas de Información en entornos de salud, habitualmente lo que se debe proteger con mayor énfasis son los datos, ya que tanto el hardware como el software son fácilmente recuperables. De todos modos se debe proteger estos dos últimos elementos ya que son el camino para atacar los datos.

7.2.1 DATOS E INFORMACIÓN

La seguridad es muy amplia, en la presente investigación estará ceñida a la protección de datos de carácter personal. En la vida cotidiana nos referimos de manera indistinta a datos e información, pero para ser más precisos tenemos que diferenciarlos.

Señala Dueñas Nogueras (2014) que la mayoría de las personas que trabajan en el procesamiento de información confunden los conceptos de dato e información. Sin embargo, se debe tener en cuenta que un dato no es más que una representación de hechos determinados que se han producido; el dato tiene un escaso valor y necesitará de una determinada interpretación para que dicho dato adquiera la capacidad de transmitir algún significado. Pero cuando se habla de información, ésta debe ser definida como el significado que un individuo asigna a un determinado dato o conjunto de datos, por lo que es un elemento que posee un valor añadido, posee un significado y será útil para la toma de decisiones y logro de objetivos.

El Reglamento de desarrollo de la Ley Orgánica 15/1999 de fecha 13 de diciembre de Protección de Datos de Carácter Personal (Real Decreto 1720/2007), en adelante Reglamento LOPD, en su artículo 5 alude diferentes tipos de datos:

> e) *Dato disociado:* aquél que no permite la identificación de un afectado o interesado.

f) *Datos de carácter personal:* Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

g) *Datos de carácter personal relacionados con la salud:* las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

Probablemente en este artículo se presenta esta diferencia por no repetir el mismo término figurando ambos en más casos en el Reglamento LOPD. La Ley Orgánica de Protección de Datos, en su artículo 3, define datos de carácter personal como: «Cualquier información concerniente a personas físicas identificadas o identificables».

Para la Real Academia Española, la palabra dato, según su acepción significa: «Antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir consecuencias legítimas de un hecho». Pero ha añadido hace años otra acepción, Informática, «Información dispuesta de manera adecuada para su tratamiento por un ordenador». Por otro lado, información es «Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada».

Si se consulta la norma ISO 27002, el anexo de la norma UNE ISO 27001, ésta habla de seguridad de la información; el punto 15.1.4 se refiere a protección de datos de carácter personal y de la intimidad de las personas.

Se consideran sinónimos ambos términos a estos efectos, salvo las diferencias que puedan haber establecido la LOPD, el Reglamento de desarrollo de la Ley Orgánica 15/1999 u otras normas vigentes o futuras. Así, en este contexto se debe hablar de seguridad de los datos (artículo 9 de la LOPD) y de la información (ISO 27001), y ya tratados en conjunto frente a otras expresiones válidas: seguridad informática, seguridad de las comunicaciones, de las TIC como tecnologías de la información y de las comunicaciones.

7.2.1.1 **Clasificación de la información**

La clasificación, por lo general, se la entiende relacionada con la confidencialidad y la integridad, incluso de forma conjunta, si bien en

muchos casos se ha de diferenciar, así todos podrán ver la Web de una entidad (salvo posibles áreas reservadas a empleados Intranet, o a distribuidores u otros, Extranet, o bien accesible solo por clientes o suscriptores), pero muy pocos podrán variar su contenido; es decir, en este caso se diferenciará confidencialidad frente a integridad, posibilidad de modificación de contenidos.

Desde la perspectiva de la norma ISO 27001, una de las medidas de seguridad que más trabajo cuesta definir e implantar en toda organización es el objetivo de control «A.7.2. Clasificación de información» que intenta asegurar que se aplica un nivel de protección adecuado a la información.

En ISO 27002, el objetivo de control A.7.2 tiene dos mecanismos de control posibles que hay que construir para lograr asegurar el tratamiento adecuado según los niveles de seguridad establecidos. Por tanto, se tienen los dos siguientes controles.

— Control A.7.2.1. Directrices de clasificación que pretende lo siguiente: «La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización».

— Control A.7.2.2. Marcado y tratamiento de la información que pretende lo siguiente: «Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización».

Las consecuencias prácticas de estos dos controles es que la organización debe establecer diferentes niveles de clasificación de la información (habitualmente representados por las etiquetas como «público», «uso interno», «confidencial», «reservado») y definir en cada nivel qué tipos de acciones o protecciones se deben tomar en cada una de las fases de tratamiento (creación, almacenamiento, distribución, transporte o destrucción) (Cao, 2013).

Pero también se puede clasificar la información y otros recursos en cuanto a su disponibilidad, según lo crítico que sea para la continuidad de la entidad, y en este caso no solo bases de datos, sino aplicaciones y comunicaciones, y en ningún caso se debería tratar de personas.

Al centrarse en la clasificación más común de los datos relacionada con confidencialidad e integridad, se encontrará que algunos posibles niveles pueden ser: de uso interno, de uso restringido, confidencial, secreto o incluso alto secreto.

La clasificación ha de tenerse en cuenta a lo largo de todo el ciclo de vida de los datos, y en el caso de resultados en papel o datos en soportes informáticos; en función de su contenido, puede ser imprescindible la destrucción total cuando no son necesarios, aspecto que recoge el Reglamento de desarrollo de la Ley Orgánica 15/1999 en cuanto a soportes.

Cuando ese activo es la información, la importancia que se le asigne dependerá de la necesidad que haya de garantizar que no sea conocida por terceros que no deben tener acceso a ella y de saber que la información que se obtiene no es parcial y se puede acceder a ella en el momento que sea necesaria, hecho que puede afectar a la toma de decisiones equivocadas o poco óptimas.

Esta información constituye uno de los valores más importantes de las empresas hoy en día, debido a la generalización en el uso de los instrumentos informáticos. Las empresas deben inventariar estos activos y dotarlos de medidas de protección y seguridad, no solo para el cumplimiento legal de requisitos, sino también para asegurar accesos deliberados no consentidos de terceros. En este sentido, se propone la siguiente clasificación:

— *Datos confidenciales:* Son aquellos datos de difusión no autorizada. Su uso puede suponer un importante daño a la organización.

— *Datos restringidos:* Son aquellos datos de difusión no autorizada. Su utilización iría contra los intereses de la organización y/o sus clientes.

— *Datos de uso interno:* Son aquellos datos que no necesitan ningún grado de protección para su difusión dentro de la organización.

— *Datos no clasificados:* Son aquellos datos que no necesitan ningún grado de protección para su difusión.

— *Datos de carácter personal:* Son aquellos datos relacionados con la intimidad de las personas y son un tipo de datos específicos que legalmente deben ser protegidos (Alonso *et al.*, 2009).

Los datos relativos a la salud de las personas han tenido siempre un carácter estrictamente confidencial, toda vez que durante un proceso asistencial el paciente puede llegar a compartir con su médico aspectos de su vida íntima que no revela a nadie más, y lo hace con la confianza de que el médico guardará absoluto secreto; pero lo hará, sobre todo, con la esperanza de que esta información sea útil para mejorar o proteger su estado de salud (Blanco y Rojas, 2012).

7.2.2 SOFTWARE

Al observar este segundo elemento a salvaguardar, se está frente a un conglomerado de programas que constituyen la estructura que permite al ordenador la ejecución de actividades. Actualmente es más importante que el propio hardware (Téllez Valdez, 2004).

Existen dos (2) tipos principales de software: el software de base o sistemas y el software de aplicación, cada uno de ellos tiene funciones diferentes. El primero es un conjunto de programas generalizados que administran los recursos al ordenador. En cambio, el software de aplicación circunscribe a los programas que son desarrollaros para los usuarios con el fin de aplicar el ordenador a una tarea específica. Ambos tipos de software están interrelacionados, el software de sistemas rodea al hardware y controla el acceso a él, en tanto el software de aplicación trabaja a través del software de sistemas para poder realizar las tareas exigidas por los usuarios finales (Amaya Amaya, 2010).

Dentro de una infraestructura tecnológica en el ámbito de la salud, la mayor cantidad del software utilizado es de aplicación (sistemas específicos, como los de registro de pacientes, prescripción médica, etc.), aunque es indispensable el software de base, necesario para el funcionamiento y control de los equipos (sistemas operativos, gestores de bases de datos, utilidades, entornos de programación y otros).

Actualmente, el desarrollo de software se basa en la programación por capas que consiste en dividir una aplicación en varios niveles independientes, de modo que un cambio en uno de ellos no suponga grandes cambios en los demás.

Dentro del software de aplicación, cuando de tratamiento de información se refiere, el elemento globalizador se denomina Sistemas de Información.

7.2.2.1 Sistemas de Información

El glosario de términos del *Information Systems Audit and Control Association* (ISACA) define a un sistema de información como «La combinación de actividades estratégicas, operativas y de gestión involucrados en la recopilación, procesamiento, almacenamiento, distribución y uso información y su tecnología» (ISACA, 2015).

Por lo que un sistema de información se puede definir técnicamente como un conjunto de componentes relacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización.

Dentro de la presente investigación, se verán los sistemas de información en el entorno sanitario, los cuales serían el segundo elemento a cuidar a la hora de establecer los parámetros de seguridad.

7.2.2.2 Sistemas de información hospitalarios

Romero Gutiérrez (2004:432) señala que la necesidad de contar con sistemas de información en las organizaciones sanitarias ha venido condicionada por tres tipos de necesidades generales:

— Necesidad de controlar el gasto (evitar costes no productivos);

— Necesidad de satisfacer a la población (facilitar mejoras), y

— Necesidad de evaluar resultados de decisiones (gestionar los cambios).

Actualmente se acepta que los sistemas de información tienden a ser, además, un instrumento esencial para satisfacer las necesidades de soporte continuo al trabajo de los profesionales. Pero este objetivo está lejos de alcanzarse.

En general se acepta que los sistemas de información son elementos subordinados del negocio, pero potenciarlos es una opción de alto valor estratégico. Hoy existen métodos de efectividad probada para

obtener la información que se puede necesitar en actividades de gestión clínica.

El HIS (acrónimo de *Hospital Information System*, Sistema de Información Hospitalario) es un sistema integrado de información diseñado para gestionar todos los aspectos clínicos, administrativos y financieros de un hospital. Además, permite obtener estadísticas generales de pacientes, datos epidemiológicos, de salud laboral y salud pública, entre otros (García, 2012).

El HIS puede estar compuesto por uno o varios componentes de software y una gran variedad de subsistemas de especialidades médicas como ser:

— Sistemas de gestión de petición de prestaciones.
— Sistemas de información de radiología.
— Sistemas de información de laboratorio Clínico, también denominado SIL.
— Sistemas de patológica digital o telepatología.
— Sistemas de Gestión de la imagen médica digital.
— Sistemas de telerradiología.
— Sistemas de gestión electrónica de la farmacoterapia.
— Otros.

7.2.2.3 **Sistemas de información para la gestión clínica**

La gestión clínica es el resultado de un encuentro voluntario entre la cultura clínica y la cultura de gestión. Todo conjunto de datos, información, conocimiento y sabiduría que ambas culturas pueden aportar se debe combinar armónicamente para introducir mejoras en los servicios de salud actuales y futuros.

Las fórmulas que cada organización usa para combinar los ingredientes son diferentes; pero en cualquier caso, unos productos y servicios de información eficaces, rigurosos, dinámicos, fiables y sostenibles pueden ser una aportación valiosa para el éxito de las iniciativas de gestión clínica.

Para que esos productos y servicios puedan llegar a ser viables y resulten efectivos, hay que contar con sistemas de características (in-

fraestructura, proceso, estándares) adecuadas a las necesidades específicas, los ciclos de trabajo y los condicionantes económicos de las organizaciones sanitarias (Romero Gutiérrez, 2004).

La gestión clínica puede considerarse un área de conocimiento médico que aplica técnicas de gestión para obtener servicios asistenciales óptimos. Como cualquier actividad clínica, abarca actividades de diagnóstico, tratamiento e información. A diferencia de la clínica, sus técnicas básicas no son biomédicas sino epidemiológicas, analíticas, organizativas, tecnológicas y económicas. Quizá sus motivaciones principales sean el espíritu emprendedor de los clínicos y la voluntad de trabajar bien por, para y con los pacientes.

7.2.2.3.1 *Sistemas de información: hacia una arquitectura de componentes intercambiables*

Para que los sistemas de información sean capaces de responder con agilidad y oportunidad a las exigencias del entorno, preservando su capacidad de incorporar los avances metodológicos y tecnológicos que se producen en forma continua, deben contar con una arquitectura de múltiples componentes intercambiables. En lugar de tender a una unificación tecnológica que los puede hacer vulnerables a cambios externos (tecnologías, proveedores, presupuesto de inversiones, estándares del sector, prioridades de política sanitaria) se debe estimular la implantación de pequeños subsistemas susceptibles de control interno o, en ciertos casos, de provisión externa con un volumen de recursos económicos limitados.

La interfaz de comunicación e información compartida entre los subsistemas será objeto de un control muy estricto por la organización, ya que es lo que permite que ninguno de los elementos sea insustituible.

En un sistema de información bien estructurado se debe considerar como hechos asistenciales susceptibles de medición, control y evaluación al menos los siguientes:

— *Demanda:* volumen, demoras, cancelaciones, reprogramaciones.

— *Demora:* retardo, espera, total, retrospectiva, prospectiva.

— *Recursos:* dotación, horario, ocupación, utilización, amortización.

— *Actividad:* tipo, distribución.

— *Flujos:* origen, destino, motivo, adecuación, fluctuaciones.

— *Producción:* tipificación, volumen, consumos, variabilidad.

— *Resultados:* supervivencia, salud, satisfacción, beneficio.

Y también hay que tener en cuenta como mínimo las siguientes dimensiones por cada hecho asistencial que se decida controlar:

— *Cantidad:* volumen, intensidad.

— *Calidad:* estructura, procesos, resultados.

— *Variedad:* cartera, cobertura.

— Coste: volumen, ratios, comparación.

— *Innovación:* ideas, recursos, soporte.

— *Evidencia:* selección, preferencias, práctica (Romero Gutiérrez, 2004).

7.2.2.3.2 *Técnicas de análisis de información*

El objetivo directo de las técnicas de análisis de la información consiste en hacer un uso óptimo de las bases de datos clínico-administrativas. La incorporación de la capacidad analítica de los paquetes ofimáticos ayuda a descentralizar la información para que sirva para la toma de decisiones.

En una situación ideal, los mecanismos de diagnóstico de gestión automatizados coexisten con sistemas de consulta personalizables, como consecuencia de ello, la búsqueda y recolección de información, el filtrado de la información relevante y la búsqueda de hipótesis explicativas de los fenómenos observados no resultan una carga de trabajo disuasoria para las personas que se incorporan a actividades de gestión.

Por lo tanto, merece la pena mencionar al menos algunas tecnologías y métodos que pueden ayudar a desarrollar con éxito sistemas de información para la gestión clínica:

— SQL *Structured Query Language* (lenguaje estructurado de consulta).

— ODBC *Open Data Base Connectivity.*

— Hojas de cálculo y tablas dinámicas.

— Repositorios de datos.

— Minería de datos y visualización de datos.

— OLAP *On-Line Analytic Processing.*

— Tablas de referencia (ficheros maestros locales, tablas de transcodificación).

— Paquetes estadísticos.

Los Servicios de Admisión y Documentación Clínica (SADC) han de afrontar a muy corto plazo un nuevo papel, orientado a facilitar la descentralización de la gestión de pacientes y a optimizar la disponibilidad de información clínico-asistencial. Sin abandonar la posición de enlace, tendrán que asumir la responsabilidad de desarrollar, sostener y anticipar una buena infraestructura de sistemas de información para directivos, profesionales y pacientes. Este es un papel emergente, pero será una de las funciones predominantes dentro de cinco años (Romero Gutiérrez, 2004).

7.2.2.3.3 *Tecnologías y sistemas sostenibles*

El hecho de que hoy se implante un sistema de información, no significa que vaya a seguir funcionando dentro de diez años, por ejemplo. Ni siquiera el hecho de que se haya dedicado un considerable esfuerzo económico u organizativo al desarrollo y puesta en marcha de un sistema permite predecir su duración. Un atributo clave de los sistemas de información es su sostenibilidad. Algunas tecnologías que hoy están disponibles, incluso a bajo coste, permiten concebir la esperanza de que los sistemas del futuro sean más sostenibles que los del pasado.

Existen algunas trabas que dificultan o interrumpen el desarrollo de los sistemas de información, entre ellas se enumeran las siguientes:

— Coste de las operaciones de producción o registro de datos.

— Métodos de procesamiento inadecuados.

— Dificultades de transferencia de información.

— Canales ineficaces de difusión del conocimiento.

— Modelos de almacenamiento incompletos.

— Diseconomías de distribución (Romero Gutiérrez, 2004).

Los sistemas de información clínica serán un aliado muy importante de los clínicos-gestores. Permitirán que la optimización de procesos no se base en trabajar con más intensidad, sino en trabajar más inteligentemente. El trabajo relacionado con búsqueda, análisis, almacenamiento, recuperación y comunicación de información ocupa una parte importante de la actividad clínica. El progresivo desarrollo de redes Intranet clínicas ha introducido cambios importantes en el manejo de la información desde hace más de cinco años y beneficiará a miles de profesionales en los próximos años.

7.2.3 HARDWARE

El hardware es concebido como el elemento físico que aloja el software y permite su funcionamiento. En sistemas tan críticos como los de Salud-e es fundamental conocer opciones como las configuraciones en alto rendimiento y alta disponibilidad, así como la virtualización de servidores.

Lógicamente la arquitectura hardware casi siempre se ve condicionada por la arquitectura del software al que debe dar soporte, por lo que se hace tan importante esta relación hasta el punto de que se replica la distinción entre servidores y clientes.

Los clientes hardware incluyen una gran variedad de equipos, como ordenadores de escritorio, ordenadores portátiles y dispositivos móviles, entre otros. Un servidor hardware es un equipo de altas prestaciones cuyas características (por ejemplo, alta capacidad de procesamiento de información y robustez) dependen siempre de la exigencia del software a ser utilizado. Por ejemplo, en el caso de los sistemas informáticos de salud, requerirá un servidor con mayor capacidad de procesamiento que pueda resistir una alta carga de actividad ya que puede contener aplicaciones con cien usuarios concurrentes y estos deben funcionar ininterrumpidamente.

Comúnmente se tiene que en un servidor puedan convivir varias aplicaciones; sin embargo, es habitual que las aplicaciones más críticas y de mayor complejidad para una organización sean instaladas, cada una, en un servidor diferente conocido como servidor dedicado.

Cabe destacar que a efectos de dimensionamiento un gestor de bases de datos se comporta como una aplicación más, y por lo tanto necesita también un servidor dedicado.

De la misma manera, es posible incrementar la robustez del sistema mediante la instalación de varios servidores para una misma aplicación para que la carga de la actividad exigida se reparta más o menos equitativamente entre ellos (configuración en clúster de alto rendimiento) o que, en caso de que se genere un error de uno de los servidores, sus tareas sean asumidas y continuadas por los demás servidores (configuración en clúster de alta disponibilidad).

Últimamente, una opción que resulta interesante y novedosa para la implantación de este tipo de configuraciones es la virtualización de servidores, el cual es un proceso en el que se crean varios servidores lógicos sobre un mismo servidor físico. La virtualización permite reducir la cantidad de servidores físicos y maximizar su aprovechamiento.

7.3 ¿DE QUÉ PROTEGER?

Una vez analizado lo que se debe proteger, es necesario señalar cuáles son los factores que inciden en el quiebre de la seguridad que se pretende establecer en todo Sistema de Información. Son muchos los actores que interactúan con los sistemas de información insertados en las actividades de los servicios de salud, cada uno de ellos representa un factor de riesgo que es necesario considerar al momento de establecer un plan de Seguridad de la información.

Como se ha visto anteriormente, es importante aplicar las TIC a la actividad clínica y de gestión de los servicios de salud; sin embargo, no es menos importante establecer mecanismos que viabilicen el correcto funcionamiento de los sistemas integrados a la salud. Las amenazas lógicas, problemas físicos, catástrofes, riesgos, vulnerabilidades son algunos de los aspectos que hay que cuidar al momento de afrontar la implementación de sistemas de información. De la misma manera, uno de los factores de riesgo más importante es el elemento humano que interactúa con los sistemas por lo que se hace necesario una gestión de cambio en los operadores y usuarios de las TIC en el ámbito de la salud.

7.3.1 EVALUACIÓN DE RIESGOS

La Guía ISO/CEI 73 de Gestión de riesgos define la gestión de riesgos de la entidad como «actividades coordinadas para dirigir y controlar una empresa en relación con el riesgo. La gestión de riesgos incluye, por norma general, evaluación de riesgos, tratamiento de riesgos, aceptación de riesgos y comunicación de riesgos».

Con estos posibles pasos resumidos se hará referencia a la evaluación de riesgos:

— Identificar los riesgos, preferentemente por parte de expertos independientes.

— Evaluación de esos riesgos, según probabilidad y pérdida estimada.

— Consideración de controles que disminuyan la probabilidad o el impacto, siendo muy difícil la eliminación de forma completa.

— Decisión acerca del riesgo residual, que puede ser el riesgo total: aceptarlo o transferirlo.

Para ello se habrán considerado los daños que pueden sufrir los activos, tanto en cuanto a pérdida de confidencialidad, integridad o disponibilidad.

La implantación de controles disminuye el riesgo, esos controles dependerán del tipo de activo a proteger y de las amenazas a que esté sometido, y pueden ser generales o más específicos, y humanos o técnicos, así como tangibles y físicos, o bien de tipo lógico.

La evaluación de riesgos ha de llevarse a cabo por parte de expertos que sean independientes, y de forma periódica, porque van cambiando las circunstancias y las amenazas. En el caso de la aceptación ha de ser a un nivel adecuado y por parte de la Dirección, no siendo los técnicos las funciones idóneas para asumir riesgos, que normalmente afectarán al negocio.

En los informes de evaluación de riesgos y de auditoría, para que se puedan fijar prioridades, no solo se indica si es un riesgo bajo, medio o alto, sino también el plazo de implantación aconsejado, el posible coste y el posible esfuerzo, para que la entidad pueda fijar prioridades y conozca el nivel de riesgo que puede tener el dilatar la implantación de medidas, cuando no es posible hacerlo a corto plazo, por falta de recursos, por ejemplo.

La transferencia del riesgo puede ser a una compañía de seguros, pero hablando de información ha de complementarse con otras medidas porque no se trata solamente de recuperar el valor económico de equipos y datos. Transferir el riesgo puede ser también contratando a un proveedor que se comprometa a unas medidas de seguridad, y con el correspondiente contrato, que es lo que se hace con un *outsourcing* o con la contratación parcial de servicios, como albergar la Web o un portal de comercio electrónico.

En España, la evaluación se hace contra el Reglamento LOPD, pero aun así diferentes evaluadores pueden llegar a conclusiones algo diferentes.

A su vez, una inspección de la Agencia de Protección de Datos (estatal o autonómica) puede fijarse en otros aspectos, o dar una importancia diferente a las debilidades que hayan aparecido en un diagnóstico o evaluación, o en una auditoría.

7.3.2 VULNERABILIDAD Y DEBILIDAD

El concepto de vulnerabilidad se define de forma ligeramente distinta según el glosario que se elija, Elvira Mifsud (2012:13) considera la vulnerabilidad como «debilidad de cualquier tipo que compromete la seguridad del sistema informático». Se usa rutinariamente como sinónimo de vulnerabilidad la debilidad que existe siempre que un ataque es posible. El término oportunidad se utiliza poco en análisis de seguridad, cuando la eliminación más efectiva de riesgos se produce al eliminar la oportunidad de que se produzcan, por ejemplo, es más efectivo que sólo los servidores imprescindibles estén activos, que configurar un cortafuegos que impida el acceso a los servicios no imprescindibles.

Para conocer la probabilidad se hacen estadísticas basadas en sucesos pasados elaboradas a partir del número de casos favorables y el número de casos posibles; faltando esta información, no es posible calcular la probabilidad, con lo que la vulnerabilidad será desconocida.

Las vulnerabilidades de los sistemas informáticos se agrupa en función de:

Diseño:

— Debilidad en el diseño de protocolos utilizados en las redes.

— Política de seguridad deficiente e inexistente.

Implementación:

— Errores de programación.

— Existencia de «puertas traseras» en los sistemas informáticos.

— Descuido de los fabricantes.

Uso:

— Mala configuración de los sistemas informáticos.

— Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.

— Disponibilidad de herramientas que facilitan los ataques.

— Limitación gubernamental de tecnologías de seguridad.

Vulnerabilidad del día cero:

— Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución «conocida», pero se sabe cómo explotarla (Mifsud, 2012).

La vulnerabilidad no solo depende de lo bien que uno se puede defender, sino también de cuánto nos atacan. Este no es el único defecto práctico del concepto de vulnerabilidad, dado que para que una probabilidad conocida tenga cierta capacidad predictiva se debe disponer de una cantidad suficientemente grande de casos, la probabilidad no tiene capacidad de predicción para casos individuales.

Al hacer una predicción mediante probabilidades se está suponiendo que el futuro se parece al pasado y que las condiciones externas no cambian. Ante la escasez de información y dadas la complejidad de comportamiento de los atacantes y de las organizaciones que utilizan sistemas de información, es aventurado suponer las condiciones externas como constantes, por lo que pocas veces se puede hacer estimaciones cuantitativas de las causas de que depende algún tipo de vulnerabilidad ante un ataque. Existen muchos factores que inciden en la vulnerabilidad a los cuales se debe prestar mucha atención.

En resumen, al hacer referencia cómodamente a las vulnerabilidades se tiene conocimiento sobre las debilidades, y se piensa en la eliminación de oportunidades como una de las medidas de seguridad más efectivas.

7.3.3 AMENAZAS

Según la ISO/IEC 13335-1:2004, la amenaza es una «causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización». Para proteger estas expectativas hay que identificar, evaluar y prever qué amenazas pueden afectar a su cumplimiento continuado, y ser capaces de mediar, sea cuantitativamente o cualitativamente, la posibilidad y probabilidad de materialización de esas amenazas.

Para Aceituno Canal (2004:25) las amenazas se pueden clasificar en tres grandes grupos:

Amenazas terciarias o directas: que son las que amenazan directamente el cumplimiento de nuestras expectativas, por ejemplo, una inundación. Las amenazas terciarias pueden clasificarse de muchas formas, una posible clasificación es dividirlas en accidentes, ataques y errores. Los ataques tienen siempre detrás a un actor con determinada motivación, medios y capacidad. Los accidentes suelen ser naturales, como puede ser un terremoto o el fallo de un disco duro por el uso. Los errores pueden ser naturales, pero también se pueden manipular, como puede ser un cracker que genera un *coredump* en un sistema que está atacando.

Amenazas secundarias: que son las que disminuyen o eliminan el grado de éxito de las medidas que se ponen para mitigar las amenazas primarias, por ejemplo defectos de un cortafuegos. Las amenazas secundarias son las relacionadas con el ciclo de vida de los activos y las medidas de seguridad. Cuando la selección, implantación u operación o pruebas de una medida es defectuosa, se puede adquirir una sensación de protección que no corresponde y en un futuro ver las expectativas incumplidas. Las amenazas secundarias y terciarias se diferencias de las primarias en que son evitables cuando la organización está capacitada para ello.

Amenazas primarias: que son las que evitan que se mantengan o lleguen a establecerse las medidas que mitigan las amenazas terciarias o secundarias, por ejemplo, organización de seguridad ineficaz. Las amenazas primarias están relacionadas con la capacidad de la organización para mantener la seguridad, estas amenazas impiden a la organización tomar medidas de seguridad efectivas. La tecnología no puede corregirlas.

Elvira Mifsud (2012:13) considera a la amenaza como «el escenario en el que una acción o suceso, ya sea o no deliberado, compromete la seguridad de un elemento del sistema informático».

Cuando a un sistema de información se le detecta una vulnerabilidad y existe una amenaza asociada a dicha vulnerabilidad, puede ocurrir que el suceso o evento se produzca y nuestro sistema estará en riesgo. Si el evento se produce y el riesgo que era probable ahora es real, el sistema informático sufrirá daños que habrá que valorar cualitativa y cuantitativamente, y esto se llama «impacto».

Integrando estos conceptos se puede decir que «un evento producido en el sistema informático que constituye una amenaza, asociada a una vulnerabilidad del sistema, produce un impacto sobre él». Si se quiere eliminar las vulnerabilidades del sistema informático o disminuir el impacto que puedan producir sobre él, se ha de proteger el sistema mediante una serie de medidas de seguridad.

7.4 **¿QUÉ CONSEGUIR?**

7.4.1 FACTORES CRÍTICOS DE ÉXITO

Como en cualquier plan, proyecto o implantación, al abordar la seguridad se pueden considerar los Factores Críticos de Éxito (FCE). La norma ISO 27001 sugiere éstos:

a) La concienciación del empleado por la seguridad. Principal objetivo a conseguir.

b) Realización de comités a distintos niveles (operativos, de dirección, etc.) con gestión continua de no conformidades, incidentes de seguridad, acciones de mejora, tratamiento de riesgos.

c) Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).

d) La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.

e) La seguridad no es un producto, es un proceso.

f) La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.

g) La seguridad debe ser inherente a los procesos de información y del negocio.

El problema de la protección de datos personales puede ser más difícil que la protección de otros activos o bienes, porque las comunicaciones y especialmente a través de Internet, cuando son los datos accesibles por este medio y no existe protección adecuada, pueden existir accesos indebidos desde cualquier parte del mundo y las 24 horas del día. Por otra parte, al contrario de lo que ocurre con otros activos, la copia tiene el mismo valor que el original, lo que es excelente pensando en asegurar la disponibilidad y a veces la integridad mediante las copias de respaldo. Pero a la vez es un riesgo añadido, porque quien logre acceder a los datos y copiarlos, y probablemente sin dejar pistas o borrándolas, tendrá el mismo valor que el original, aunque con el tiempo la copia pueda perder actualidad.

7.4.2 MEDIDAS ENCAMINADAS PARA GARANTIZAR LOS NIVELES DE SEGURIDAD

Dentro de la seguridad de la información se pueden tener 2 tipos de seguridad: la seguridad física y la seguridad lógica.

La «seguridad física» de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema. Las principales amenazas que se prevén son:

— Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales.

— Amenazas ocasionadas por el hombre como robos o sabotajes.

— Disturbios internos y externos deliberados.

Evaluar y controlar permanentemente la seguridad física del sistema es la base para comenzar a integrar la seguridad como función primordial del mismo. Tener controlado el ambiente y acceso físico

permite disminuir siniestros y tener los medios para luchar contra accidentes.

En cambio la «seguridad lógica» de un sistema informático consiste en la aplicación de barreras y procedimientos que protejan el acceso a los datos y a la información contenida en él.

El activo más importante de un sistema informático es la información y, por tanto, la seguridad lógica se plantea como uno de los objetivos más importantes.

La seguridad lógica trata de conseguir los siguientes objetivos:

— Restringir el acceso a los programas y archivos.

— Asegurar que los usuarios puedan trabajar sin supervisión y no puedan modificar los programas ni los archivos que no correspondan.

— Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.

— Verificar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y que la información recibida sea la misma que la transmitida.

— Disponer de pasos alternativos de emergencia para la transmisión de información.

Bajo este antecedente, Ruiz (2008) señala 8 medidas encaminadas a garantizar los niveles de seguridad para cualquier empresa en general:

1. Identificación y autenticación del personal autorizado a acceder a los datos personales:

a) *Medidas de seguridad fís*ica: éstas se realizan a través de diferentes actividades como ser, la gestión del acceso físico por llave única o el control de acceso por adjudicación de llaves codificadas.

b) *Medidas de seguridad ló*gica: a través de, asignación de identificadores a cada tipo de usuario (usuario estándar o usuario privilegiado).

2. Control de acceso:

a) *Medidas de seguridad fís*ica: distribución de autorizaciones para el acceso a los soportes físicos donde se encuentre la información. Esta distribución dependerá del nivel de seguridad exigido para cada fichero.

b) *Medidas de seguridad lóg*ica: mediante la asignación de contraseñas y el registro de los accesos a los ficheros por parte de todos los usuarios.

3. Gestión de soportes: Medida que se implementa a través de la identificación, inventariado y almacenamiento de soportes informáticos con datos de carácter personal. En esta medida también se debe hacer el seguimiento al control de entrada y salida de soportes.

4. Accesos a datos a través de redes de comunicaciones: La interconexión de sistemas a través de redes hace, muchas veces, más fácil el acceso ilegal a la información contenida, por lo que se hace necesario restringir y controlar el tránsito que existe a través de la red.

5. Régimen de trabajo fuera de los locales de la ubicación del fichero: Este régimen debe ser autorizado expresamente por el responsable del fichero y debe garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

6. Ficheros temporales: Estos ficheros deberán ser borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

7. Copias de seguridad: Deberá existir un procedimiento de recuperación de los datos contenidos en los ficheros. El responsable del sistema u otro usuario autorizado realizará una copia de seguridad periódicamente a efectos de respaldo y posible recuperación en caso de fallo. Se debe tener en cuenta también los medios físicos para efectuar las copias de seguridad y el lugar de custodia.

8. Pruebas con datos reales: Las pruebas de ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al fichero tratado.

7.5 ¿CÓMO PROTEGER?

7.5.1 ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Existen docenas de estándares y metodologías para seguridad en sistemas de información, entre ellos:

— UNE-ISO/IEC 27000 series, basado en el ISO 17799.

— La RFC 2196 del *Internet Engineering Task Force*.

— COBIT de la ISACA.

— GAISP-Principios generalmente aceptados de seguridad de la información, desarrollado por ISSA.

— GAO/AIMD-12.19.6 del *Federal Information Security Foundation*.

— ISM3 – *Information Security Management Maturity Model*.

— El *Standard of Good Practice for Information Security* del ISF.

— HIPAA, *Health Insurance Portability and Accountability Act*.

Muchos de éstos han ganado un grado de la aprobación dentro de la comunidad internacional de seguridad de información y cada uno añade valor a la inversión de seguridad de información. Aunque es necesario aclarar que varios de éstos no fueron diseñados respaldar la seguridad de información específicamente, muchos de los procesos dentro de estas prácticas respaldan los aspectos diferentes de la confidencialidad, la integridad, y la disponibilidad.

7.5.2 TECNOLOGÍAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Las tecnologías suelen ser distintas dependiendo de si se protege información, mensajes, entrada/salida o infraestructura.

7.5.2.1 **Documentar las medidas de seguridad**

Las organizaciones observan la necesidad de documentar, desde luego es imprescindible determinar qué actuaciones son críticas y por tanto necesarias que estén cuidadosamente detalladas y controladas, cuáles lo son en menor medida o aquellas en las que por su mínimo riesgo y mayor urgencia requieren de medidas flexibles. Lo crítico de las actuaciones a realizar estará en función de la importancia que tenga la protección al que va dirigida esa acción.

Hay que tener en cuenta que en el ámbito de una organización, desde el punto de vista de la seguridad, se pueden entender dos enfoques: la protección de la información y la continuidad del negocio.

En ocasiones el informático se queja que le corresponda precisamente esta labor, estando en realidad más relacionada tanto con el área organizativa como con la jurídica; sin embargo, se ha de tener en cuenta que en gran medida se trata de procedimientos técnicos que requieren un determinado nivel de conocimientos, mismos que deben ser una labor conjunta.

Para que una documentación sea adecuada debe estar orientada a los objetivos que desea cumplir, es decir, su aplicación a la adecuada ejecución de un conjunto de tareas. Desde un punto de vista formal debe ser: homogénea, estructurada, concisa y comprensible. Desde el punto de vista material debe contener: ámbito, objeto, alcance y desarrollo.

Para Jorge Molet (2015) determinar las medidas de seguridad al interior de la empresa, se deben tomar en cuenta factores como: (i) El riesgo inherente por tipo de dato personal; (ii) La sensibilidad de los datos personales tratados; (iii) El desarrollo tecnológico; (iv) Las posibles consecuencias de una vulneración para los titulares; (v) El número de titulares; (vi) Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; (vii) El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión; y (viii) Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al Responsable.

Al determinar lo anterior, el Responsable deberá considerar, documentar y actualizar recurrentemente acciones tales como:

a) La elaboración de un inventario de datos personales y de los sistemas de tratamiento;

b) Documentar las funciones y obligaciones de las personas que traten datos personales;

c) Contar con un análisis de riesgos de datos personales;

d) Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;

e) Realizar el análisis de brecha;

f) Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes;

g) Llevar a cabo revisiones o auditorías;

h) Capacitar al personal que efectúe el tratamiento; y

i) Realizar un registro de los medios de almacenamiento de los datos personales (Molet, 2005).

7.5.2.2 **Software y sistemas seguros**

El software es el activo que sirve para ofrecer los servicios de información de la organización. Para mantener la seguridad del software desarrollado, los requerimientos de seguridad deben ser parte integral del ciclo de desarrollo, desde la toma de requerimiento hasta la implantación.

Cuanto más seguro sea el sistema por diseño, menos medidas de seguridad se van a necesitar. La construcción de software seguro implica evitar todas las prácticas de programación que conducen a debilidades en el software (Aceituno Canal, 2004).

Para el desarrollo de software seguro se deberá tomar en cuenta algunas consideraciones como las siguientes:

— Toma de requerimientos.

— Selección y adquisición.

— Análisis.

— Diseño.

— Construcción de *software* seguro.

— Pruebas.

— Implantación.

— Mantenimiento.

7.5.2.3 **Eliminación de oportunidades: cortafuegos, *proxies***

Físicamente es posible eliminar la oportunidad de una amenaza simplemente eligiendo la localización donde esa amenaza no esté presente; por ejemplo, un Centro de Proceso de Datos (CPD) en un tercer piso no debería verse nunca afectado por el desbordamiento de un río cercano.

Un cortafuegos es un dispositivo que filtra los mensajes o conexiones que pasan a través de él. Aunque existen muchos otros protoco-

los, se hará referencia solo a los protocolos IP por ser los utilizados en Internet. Dependiendo si el protocolo proporciona una conexión fiable o no fiable se utilizan protocolos con estado o sin estado. Los cortafuegos que no son capaces de filtrar, dependiendo del estado de la conexión, se llaman filtros de paquetes. Cuando el cortafuegos es capaz de examinar no solo el estado sino el contenido de los paquetes, verificando que es aceptable para la aplicación a que está destinado, se llama *proxy*. Este filtrado es específico para cada aplicación (Aceituno Canal, 2004).

Los cortafuegos se pueden utilizar tanto para controlar la conexión entre la organización e Internet, como entre distintas zonas dentro de la organización. Los cortafuegos y *proxies* eliminan oportunidades de incidentes gracias a que bloquean el acceso a puertos, o bien controlan que las conexiones están autorizadas. Un cortafuegos también disminuye la vulnerabilidad ante ataques IP.

7.5.2.4 **Redundancia**

Se utiliza redundancia para eliminar los puntos únicos de fallo y para emplear de forma fiable canales o medios que son inherentemente poco fiables. Un punto único de fallo es aquel cuyo fallo implica el fallo del sistema, de modo que las probabilidades de fallo de un sistema son al menos tan altas como las del punto único de fallo más débil del sistema. Es por esto que cuando se tienen expectativas altas respecto de la fiabilidad de un sistema, la eliminación de puntos de fallo único es el principal camino a seguir.

Los inconvenientes de esta técnica son su coste directo, la dificultad de administración que implica invariablemente, y que los sistemas muy redundantes son al mismo tiempo muy complejos. Es por esto que sea una técnica que suele aplicarse solo a los activos críticos de la organización. La redundancia minimiza el impacto de un incidente, pero no disminuye la vulnerabilidad del sistema ante cualquier amenaza (Aceituno Canal, 2004).

Existen distintas formas de aplicar esta técnica, dependiendo de las expectativas que se tengan en la recuperación del fallo, si la recuperación no se debe notar, o si se puede tardar minutos, horas o días. Se puede aplicar redundancia tanto de proceso como de almacena-

miento, comunicación y entrada/salida. La redundancia aplicada con más frecuencia es la doble, aunque en algunos casos se aplican redundancias mayores.

7.5.2.5 **Copia de respaldo *(Backup)***

La seguridad de los datos personales de la base de datos no sólo supone la confidencialidad de los mismos, sino que también conlleva la integridad y la disponibilidad de esos datos. Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos de la base de datos.

Existirá una persona, bien sea el responsable del sistema o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad de la base de datos, a efectos de respaldo y posible recuperación en caso de fallo. Estas copias deberán realizarse con una periodicidad, al menos semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

El encargado del tratamiento obtendrá una copia de seguridad. Esta copia de seguridad será entregada al Responsable de Seguridad, quien la guardará en los armarios ignífugos situados en una habitación aislada en el *parking*, donde sólo tendrá acceso autorizado además del propio responsable de seguridad, el administrador del sistema.

En caso de fallo del sistema con pérdida total o parcial de información de la base de datos, el encargado de realizar las copias de seguridad, previa autorización del administrador del sistema, procederá a recuperar los datos contenidos en la última copia de respaldo (Ruiz Carrillo, 2008).

Finalizado el procedimiento se dejará constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

El proceso de copia de seguridad debe tener en cuenta los siguientes detalles:

— El procedimiento que se siga para su realización dependerá del modelo de arquitectura empleado. Cuanto mayor sea el grado de centralización del sistema, menos esfuerzo será necesario.

— La copia de los datos debe almacenarse en una ubicación distinta de la que alberga los datos originales y contar con las mismas medidas de protección que estos. De poco sirve proteger la información si existe una copia que presenta una vulnerabilidad mucho mayor. Este requisito se aplica no solo a las copias de respaldo, sino a cualquier copia que pueda existir con otros fines.

— Hay que realizar periódicamente simulacros de recuperación de la información, a fin de garantizar que las copias se estén generando correctamente (Martínez Santiago y Rojas de la Escalera, 2014).

La copia de respaldo es una de las tecnologías más efectivas para reducir el impacto de incidentes. Mediante copia de respaldo es posible recuperar la información, configuraciones e incluso sistemas completos. Lamentablemente realizar copias de respaldo efectivas y que pueden recuperarse con facilidad requiere un gran esfuerzo de administración.

7.5.2.6 **Control de accesos lógico y físico: directorios, medios de autenticación, registros de acceso (LOG)**

El control de accesos consiste básicamente en la capacidad de controlar y conocer quién y cuándo gana acceso, sea una zona de un edificio, a cierta información, a un mensaje o a un servicio. El control de accesos es posible que sea la medida de seguridad más importante que se puede establecer, dado que un control de accesos bien aplicado nos permite saber quién ha hecho qué, dónde y cuándo y controlar quién puede acceder a qué, dónde y cuándo, colmando las expectativas más exigentes de control sobre los activos (Ruiz Carrillo, 2008).

En el ámbito de los sistemas de información el control de acceso físico no es menos importante que el control de accesos lógico. Tanto el acceso a las salas en que se gestionan y explotan los sistemas de

información, como la fijación de los equipos que son susceptibles de robo, como la identificación de los equipos y el control de acceso a la consola necesitan con mucha frecuencia estar estrictamente controlados.

Las tecnologías de control de accesos lógicos permiten la gestión del ciclo de vida de las credenciales y la concesión de sesiones mediante autenticación, autorización y registro de uso.

Las tecnologías de control de accesos físico utilizan principalmente barreras, guardas de seguridad y tarjetas de acceso con fotografía difíciles de falsificar.

7.5.2.6.1 *Directorios*

Los directorios son la clave de cualquier sistema de control de accesos en entornos medianos y grandes. Cuando el control de accesos está basado en servidores individuales, el coste de gestión del sistema crece rápidamente según aumenta el número de servidores. El directorio centraliza el control de accesos, como un paraguas que cubre todos los sistemas operativos, servidores y otros recursos de la organización. Los principales directorios actualmente son LDAP, *Active Directory* y *eDirectory*.

Cuando en una organización existen varios directorios, se recurre a diversos parches cuando no es posible consolidarlos en uno sólo, como puede ser el uso de metadirectorios, sistemas *single sing on*, que actúan como intermediarios entre los usuarios y los distintos directorios, o incluso bases de datos manejadas por un operario, que se encarga de asegurar que las credenciales están sincronizadas en los distintos directorios existentes (Aceituno Canal, 2004).

Los sistemas de directorios son enormemente complejos, se resaltarán algunas características que son de interés en la presente investigación como:

— Un diseño del árbol de objetos representa bien la estructura orgánica o geográfica de la organización.

— El uso de protocolos complejos, como LDAP, permite garantizar el secreto de la información manejada en la autenticación y autorización, y otras operaciones.

— El soporte para cifrado permite manejar firmas electrónicas, certificados, etc.

— El soporte de medios de autenticación permite aceptar contraseñas, tarjetas inteligentes, biometría y otros medios de autenticación.

7.5.2.6.2 *Medios de autenticación*

El proceso de autenticación consiste en la comprobación de la identidad del actor, mediante la comparación del medio de autenticación que proporciona el usuario con la copia o prueba de conocimiento de este medio de autenticación que se almacena en el sistema.

En este sentido el Instituto de Tecnologías de la Comunicación (2012) ha elaborado una «*Guía sobre riesgos y buenas prácticas en autenticación online*», con el objetivo de informar sobre mecanismos de identificación y verificación de la identidad y que al utilizarlos cumplan con su función respetando los derechos de los implicados.

Existe un número muy amplio de medios de autenticación como:

— *Contraseñas:* la clave que conoce el usuario y es secreta. El principal inconveniente de este sistema es que exige al usuario recordar una o varias contraseñas, lo que lo induce a utilizar contraseñas fáciles de recordar, a repetirlas en diferentes aplicaciones, e incluso anotarlas en lugares de fácil acceso. La solución a este problema es dotar al profesional de una contraseña única para acceder a todos los sistemas corporativos y que este tome conciencia y se comprometa a la protección de dicha contraseña.

— *Frase de paso:* es como una contraseña, pero más larga.

— *Preguntas mágicas:* es una pregunta personal cuya respuesta solo debe ser conocida por el usuario, es incluso más efectiva si la respuesta que se ha elegido no está relacionada con la pregunta.

— *Tarjetas inteligentes:* son tarjetas con microchip que pueden almacenar una determinada cantidad de datos, cuya introducción en un lector permite acceder al sistema y firmar digitalmente los documentos clínicos. Normalmente requieren,

además de la inserción de la tarjeta, la introducción de una contraseña (Martínez y Rojas, 2014).

— *Token de seguridad:* un dispositivo físico que permite generar contraseñas de acceso con una validez temporal. En cierto modo puede considerarse como una combinación de contraseña y tarjeta chip.

— *Biometría:* puede hacerse biometría de la voz, el iris, la letra, la cara, las huellas digitales o los intervalos de tiempo entre las letras cuando tecleamos en un teclado. Estos intervalos son característicos de cada persona.

El inconveniente es que algunos de estos medios exigen lectores especiales que los hacen muy caros.

El proceso de autenticación por lo general se da una vez que el usuario ha realizado el registro inicial en un sistema, el administrador de dicho sistema requerirá acreditar su identidad cuando quiera acceder al mismo. De este modo se evita que personas no autorizadas accedan a estos servicios o que alguien pueda hacerse pasar por un usuario legítimo suplantando su identidad. Es lo que se denomina autenticación.

La autenticación puede realizarse de dos modos distintos, la verificación y la identificación, en función de la información que tenga que aportar el usuario. La verificación se trata del procedimiento más habitual, en ella la persona que quiere acceder al sistema debe señalar qué usuario registrado es (mediante un nombre de usuario, una cuenta de correo electrónico o el método que se determinase en el registro) y presentar sus credenciales de acceso (contraseña, elemento físico o rasgo personal). Dicho de otro modo, el usuario indica quién es y lo demuestra de la forma establecida.

Así, el sistema únicamente debe verificar que ambos elementos coinciden en sus bases de datos, es decir, que las credenciales de acceso presentadas son las mismas que se han registrado previamente para el usuario señalado.

En caso de que ambas informaciones concuerden se considerará que la persona que pretende acceder al sistema es realmente el legítimo usuario y se permitirá dicho acceso. En caso de que no coincidan la respuesta dependerá de lo establecido por el administrador del sistema, siendo lo más habitual solicitar que se repita el intento de acce-

so. En caso de que la incongruencia se produzca repetidas veces, es posible que el administrador determine un bloqueo automático de la cuenta y abra una nueva posibilidad de acceso, ya sea utilizando una autenticación basada en conocimientos (al realizar preguntas cuya respuesta debería conocer únicamente el legítimo usuario) o una autenticación basada en la posesión (por ejemplo enviando un mensaje a una cuenta de correo electrónico o un número de teléfono previamente vinculados).

Este segundo tipo de procedimiento, la identificación, es más sencillo para el usuario, pero mucho más complejo para el propio sistema al requerir mayores capacidades de computación. En él, el usuario en lugar de aportar dos tipos de informaciones solamente aporta sus credenciales. Así, el sistema es el encargado de identificar qué usuario registrado es el que se está autenticando.

Este procedimiento consiste en la comparación de las credenciales que aporta el usuario con todas las registradas en el sistema, lo cual implica mayores necesidades en la capacidad de computación del sistema y un mayor tiempo de espera para realizar la identificación.

Debido a los diversos problemas que podría acarrear este método en cuanto a las posibilidades de suplantación de identidad, es poco corriente, y en caso de ser utilizado únicamente lo sería en sistemas que basan las credenciales en la posesión de elementos físicos o en los rasgos físicos, siendo este segundo caso el que mayor seguridad aportaría (INTECO, 2012).

En consecuencia, la autenticación comprende tanto los accesos físicos como los lógicos, y se aplica a profesionales y a pacientes. En el caso de los profesionales, su autenticación no solo es un requisito para el acceso a la información, sino también una medida para garantizar el no repudio de sus acciones. De este modo, la autenticación protege tanto la confidencialidad como la integridad de los datos clínicos.

En lo relativo a los pacientes, es necesario comprobar su identidad no solo cuando acuden a la consulta, sino también cuando recogen recetas médicas y resultados de pruebas o solicitan una cita previa, sea telefónicamente o vía Internet. Los procedimientos actuales no son muy rigurosos y se limitan a la presentación de la tarjeta individual facilitada por el servicio de salud o a la petición del código de paciente, que puede deducirse a partir de datos como el nombre, los

apellidos o su fecha de nacimiento. Además, la posibilidad de delegar algunas de estas tareas en un familiar supone una dificultad adicional para la gestión de la seguridad (Martínez y Rojas, 2014).

7.5.2.6.3 *Registros de acceso (LOG)*

El registro de accesos, permite conocer quién ha accedido a los datos, cuándo lo ha hecho y qué acciones ha realizado. En otras palabras, así como la definición de permisos especifica lo que un usuario puede hacer en teoría, el registro de accesos muestra lo que dicho usuario ha hecho en la práctica (Boyle y Panko, 2013).

De este modo se garantiza la trazabilidad del sistema, lo que permite la realización de auditorías para reconstruir los pasos de los usuarios hasta cierto punto. El registro podría notificar de forma automática los accesos que incumplieran las condiciones establecidas, a fin de investigar si están debidamente justificados.

Muchas aplicaciones, sistemas operativos y elementos red utilizan *logs* para registrar el uso que se hace de ellos, y los posibles errores en el sistema. Algunos *logs* están asociados a sesiones, lo que permite rastrear el origen, otros simplemente registran eventos del sistema.

Un *log* que no se analiza no sirve apenas para nada. Debido al coste de gestión de este análisis, se debe balancear ese coste con los posibles beneficios, y contemplar medidas como adquirir programas que faciliten el análisis, seleccionar cuidadosamente de qué eventos quiere tenerse registro y centralizar los *logs* en un único directorio en una máquina dedicada (Aceituno Canal, 2004).

Gracias a los *logs* se puede hacer un análisis forense de lo sucedido en un sistema y obtener estadísticas. El *log* de un cortafuegos o un IDS[94] puede ser especialmente revelador.

Algunos profesionales asumen que un registro de accesos recoge las acciones de los usuarios hasta el más mínimo detalle. En tal caso, estos registros podrían llegar a suponer un volumen de datos mayor que el de la propia información clínica. Por lo tanto, un registro de accesos debe diseñarse de modo que su nivel de detalle garantice un

---

[94] IDS *(Intrusión DetectionSystem)* Sistema de detección de intrusos.

equilibrio razonable entre la trazabilidad de los procesos y la manejabilidad del propio registro (Martínez y Rojas, 2014).

7.5.2.7 **Cifrado**

El cifrado es la técnica de seguridad más popular, hasta el punto de que seguridad y cifrado se han convertido en sinónimos. Para simplificar, al hablar de *cifrado* se usará el término mensaje para referirse tanto a un conjunto de datos ordenados que se transmiten como a un conjunto de datos ordenados que se almacenan.

Es imposible vivir en sociedades avanzadas sin recurrir cotidianamente al cifrado, aunque sea inadvertidamente:

— Recibir una llamada por un celular.

— Conectarnos a la computadora e introducir una contraseña.

— Iniciar una sesión en internet con un servidor seguro.

— Operación en un cajero automático.

— Efectuar una compra con una tarjeta de crédito o de débito, etc.

Cifrar es una operación reversible por la que un mensaje se convierte en un conjunto de datos cuasi aleatorios, el mensaje cifrado. Como entradas de esta operación se utilizan el mensaje y la clave. La clave sirve para hacer el número de posibles cifrados distintos del mismo mensaje muy grande, dificultando la obtención del mensaje original a partir del mensaje cifrado cuando se carece de la clave. Cuanto más aleatorio sea el mensaje cifrado y mayor es el número de claves posibles, mejor es la cifra.

De un lado, cifrar una información consiste en convertir un texto en claro, esto es, datos que no han sido cifrados o que si lo han sido, han sido descifrados, en un texto ininteligible o cifrado; es decir, en una información que no se puede comprender sin la ayuda de la clave y el procedimiento adecuado para cifrarla. Por otro lado, descifrar una información consiste en convertir un texto ininteligible en un texto en claro.

El cifrado no se basa en el secreto del algoritmo de cifrado, sino en la dificultad computacional del descifrado cuando no se tiene la clave. Una operación se considera computacionalmente difícil cuando la capacidad de proceso y almacenamiento necesarios aumentan mucho

más rápido que la cantidad de datos tratados. Las operaciones de cifrado se suelen clasificar dependiendo de si utilizan una clave igual o distinta para cifrar y descifrar los datos. El cifrado simétrico usa la misma clave, el cifrado asimétrico una distinta (Aceituno Canal, 2004).

Los mecanismos que utilizamos para cifrar y descifrar serán las llamadas claves, que se asimilan a números de gran longitud para que sean seguras y que siguen un algoritmo matemático. Las mencionadas claves pueden ser generadas por un sistema informático del usuario, o bien por un sistema central que las transportará más tarde al sistema del usuario en forma segura, en este segundo caso una vez creadas y transportadas serán destruidas (Martínez Nadal, 2014).

Básicamente, se utilizan dos técnicas para encriptar y desencriptar. De modo que se distingue básicamente entre la denominada técnica de cifrado simétrico, también conocida como cifrado en clave convencional, secreta, privada, criptografía de clave simétrica, y por otro lado la técnica de cifrado asimétrico, identificada también como de clave pública, criptografía de clave asimétrica.

La primera de ellas es una técnica sencilla donde tanto emisor como receptor del mensaje del mensaje comparten una única clave que permitirá cifrar y descifrar la información.

El algoritmo de clave simétrico más utilizado es conocido como DES, *Data Encryption Standard* (estándar de cifrado de datos) que tiene como finalidad proporcionar confidencialidad en las comunicaciones.

Existe un enorme número de algoritmos de cifrado, tanto simétricos como asimétrico y para la generación de *hash*.

Los algoritmos pueden ser de bloque, lo que indican que cifran la información dividiéndola previamente en bloques, o de flujo, que indica que la información es cifrada según se procesa bit a bit. Algunos de los más populares son RSA (asimétrico), *Diffie-Hellman* (asimétrico), AES, DES, *Blowfish*, IDEA, *Rijndael* y *Skipjack*, RC4 (flujo), SHA-1 (*hash*) y MD5 (*hash*).

7.5.2.8 **Reserva**

La técnica de reserva consiste en almacenar suficiente cantidad de un suministro para soportar la interrupción de éste durante un tiem-

po razonable. Una SAI es una aplicación de la técnica de reserva, como lo es el almacenamiento de piezas de repuesto, el represamiento de agua o el uso de un *buffer* que impida la interrupción de la comunicación en caso de fallos puntuales en la línea, no es útil para interrupciones demasiado prolongadas de un suministro (Aceituno Canal, 2004).

7.5.2.9 **Almacenamiento seguro**

Cuando se requiere de una seguridad muy alta, se puede cuestionar si el disco de una computadora personal es el medio apropiado para almacenar los certificados emitidos por las Entidades de Certificación y, principalmente la clave privada de los algoritmos asimétricos, pieza clave para definir la seguridad del sistema.

Normalmente, cuando un navegador crea un par de claves, la clave privada se guarda encriptada en el disco rígido de la computadora personal. Es sabido que los *hackers* tienen diferentes métodos para hacerse de información almacenada en el disco rígido, y bien ésta no se encuentra en claro, se podría suponer que se podrían detectar fallas de código en los navegadores, o adivinar o reducir la forma en que éstos encriptan las claves privadas.

Se puede también almacenar la clave privada en un disco removible, que se coloca en la máquina solo en el momento en que se requiera acceso a la calve privada. Pero se puede pensar que precisamente en ese momento es cuando el programa hostil de un *hacker* podría actuar, extrayendo la información del disco o robándola mientras los programas la utilizan.

Otros dispositivos externos a la computadora pueden recibir programas Java descargados, para realizar por el usuario las funciones criptográficas. Pero así se permite la descarga de aplicaciones «buenas» a estos dispositivos, también podrían descargarse programas hostiles.

Parece entonces que la solución óptima como medio de almacenaje de la clave pública y los certificados digitales sería un dispositivo externo al computador, que pueda procesar la criptografía necesaria para asegurarnos que la clave pública nunca sale al exterior, al cual no se le pueden descargar programas hostiles.

La industria presenta un par de soluciones disponibles comercialmente, los *tokens* y las tarjetas inteligentes, o *smartcards*. En realidad *tokens* y *smartcards* son similares, incluso a veces el mismo circuito integrado se coloca en ambos, solo difieren en la forma física, y en la forma y protocolo con la cual se comunican con el computador. A estas soluciones se les suele llamar «Certificados almacenados en hardware» (INTECO 2012).

7.5.2.9.1 *Tarjetas Inteligentes*

Las tarjetas inteligentes hace décadas que se encuentran cumpliendo un rol en la sociedad moderna. Ya sea que almacenan datos de identidad, monetarios, de pasajes en medios de transporte, entre otras. El formato físico, similar a una tarjeta de crédito, su relativamente gran capacidad de almacenaje, pero por sobre todo su capacidad de proceso de datos en forma autónoma.

Existen en el mercado tarjetas inteligentes que tienen incorporado un coprocesador matemático programado para realizar el algoritmo RSA y las funciones *Hash*. Es más, algunas de ellas pueden generar el par de claves pública y privada para el algoritmo RSA en forma autónoma, por lo que la clave privada nunca deja la tarjeta, ni siquiera en el momento de generación. Solo la clave pública puede ser leída por el computador, para comenzar el proceso de solicitud del certificado.

Una vez obtenido, el certificado puede almacenarse en la tarjeta inteligente que posee una estructura de datos similar a los directorios de las computadoras. Esta separación de datos permite que se almacenen más de un certificado, y más de un juego de claves pública y privada.

El procesador de las tarjetas inteligentes para PKI puede verificar firmas, en forma autónoma, basta con pasar un certificado recibido para que utilice la clave pública del certificado para verificar una firma remota, por ejemplo. También pueden firmar bloques de datos utilizando la clave privada almacenada. También posee el código necesario para generar claves simétricas de sesión, pudiendo cifrar y descifrar datos con algoritmo DES.

La movilidad propia de su formato físico la hace apta para que el usuario pueda operar con su certificado y su clave privada en más de

una computadora, en el trabajo, el hogar, o en un cibercafé. Poseen funciones de control de acceso a datos e instrucciones, que sólo son activadas si se coloca un número de identificación personal (PIN). Esto es opcional, pero de activarse resuelve el problema de robo o extravío de la tarjeta inteligente (y el certificado y la clave privada que lo contienen).

Por su capacidad de almacenar datos, podría también contener datos biométricos, que podrían ser comparados dentro de la tarjeta y mediante algoritmos corridos en forma autónoma por su procesador, una vez que un lector de huellas digitales, por ejemplo, pase los datos a la tarjeta (INTECO 2012).

Resulta claro que las tarjetas inteligentes son un medio poderoso de identificación. Son algo que se tiene (la tarjeta), algo que se sabe (el PIN), y algo que es (mediante el análisis de datos biométricos), además son portátiles.

Otra característica interesante es que poseen capacidad multifunción. Esto significa que la misma tarjeta puede servir para varias funciones. Por ejemplo:

— Podría utilizarse como medio de identificación en internet (con su juego de claves, su certificado, su proceso RSA, hash y DES).

— Podría utilizarse como monedero electrónico, para hacer micropagos en el mundo real o el virtual, mediante el almacenaje y proceso seguro de un saldo, *off line* del banco.

— Podría utilizarse para el pago de transporte, como control de acceso al edificio, etc.

7.5.2.9.2 *Uso de Certificado a Nivel IP (IPSec)*

Un grupo internacional de trabajo organizado bajo el IETF ha desarrollado un método para asegurar las comunicaciones IP. Ellos lo llaman el conjunto de protocolos de Seguridad IP (IPSec).

El conjunto de protocolos IPSec está basado en tecnologías de encriptación, y agrega servicios de seguridad a la capa de red de una manera que es compatible con los estándares IP existentes (IPv4), y el cuál será obligatorio en la versión que viene (IPv6).

Esto significa que si se utiliza el conjunto de IPSec donde normalmente se usaría IP, se aseguran todas las comunicaciones en la red para todas las aplicaciones y para todos los usuarios de una forma más transparente que si se usara cualquier otra normalización.

Con IPSec se puede construir una Red Privada Virtual (VPN) una red privada segura que es tan confiable como una red de oficina aislada, pero construida en una red pública insegura. Con IPSec se puede crear una VPN segura en cualquier momento, por demanda y con cualquiera que también esté usando el estándar.

Pero debido a que IPSec trabaja con el estándar IP actual y futuro, todavía se puede usar en el medio redes IP regulares para transmitir datos. Cada extremo de la comunicación (transmisor y receptor de la información) debe cumplir con IPSec, mientras que el resto de la red puede o no trabajar con este conjunto de protocolos.

La efectividad fundamental de la normalización del grupo de IPSec es que la seguridad trabaja a un nivel bajo de la red. Lo mismo que IP es transparente para los usuarios, lo son los servicios de seguridad basados en IPSec, servidores que no se ven, funcionando en el trasfondo, aseguran que las comunicaciones sean seguras.

Al igual que la potencia y flexibilidad de IP lo hacen universal, IPSec promete convertirse en el estándar internacional, respondiendo a diversos rangos de necesidades de seguridad, permitiendo diferentes redes alrededor del mundo para la interconexión y comunicación segura.

Y al igual que IP provee servicios en redes de cualquier tamaño, desde redes de área local con miles de nodos hasta redes globales con millones, IPSec promete escalabilidad sin problemas, servicios sencillos y confiables, aunque hace más complejas las necesidades de seguridad (Internet Society, 2009).

7.5.3 REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999

La Ley Orgánica 15/1999, ha nacido con una amplia vocación de generalidad, prevé en su artículo 1 que «tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal». Compren-

de por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal. En este sentido, se vio la necesidad de promulgar el Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal, que deroga al Real Decreto 994/1999, de medidas de seguridad de los ficheros automatizados que contengan datos personales.

A los efectos de analizar las consecuencias para la regulación de la protección y tratamiento de datos de carácter personal que tiene la Ley 41/2002, interesa analizar cuál es la distinción entre medidas de seguridad técnicas y organizativas en dicho Real Decreto 1720/2007 (en adelante Reglamento de desarrollo de la LOPD). En esta norma reglamentaria se establecen tres niveles de medidas de seguridad: básico, medio y alto.

A continuación (vamos a ver) *se verá* cada una de ellos:

— *Nivel básico:* cualquier organización que disponga de un fichero que contenga datos de carácter personal, aunque no se trate de datos calificados por la LOPD como de especialmente protegidos, deberá elaborar un Documento de Seguridad, y no solamente organizaciones tanto públicas como privadas y organizaciones administrativas, sino también profesionales y empresarios que mantengan este tipo de ficheros en el ejercicio de su actividad.

— *Nivel medio:* deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio los ficheros que contengan datos relativos a:

  • La comisión de infracciones administrativas o penales.

  • Hacienda Pública, entendidos como tales los contenidos en ficheros titularidad de la Agencia Tributaria y organismos con competencias en materia tributaria.

  • Servicios financieros, entendidos como tales los contenidos en ficheros de titularidad de entidades dedicadas a la prestación de este tipo de servicios.

  • La prestación de servicios de solvencia patrimonial y crédito.

— *Nivel alto:* además de las medidas de nivel básico y medio, adoptarán las calificadas de nivel alto los ficheros que contengan datos de:

- Ideología.
- Religión.
- Creencias.
- Origen racial.
- Salud.
- Vida sexual.
- Recabados para fines policiales sin consentimiento de las personas afectadas.
- Afiliación sindical.

Tabla 12. Elaboración e implantación de medidas de seguridad

Medidas de seguridad exigibles	Nivel Básico	Nivel Medio	Nivel Alto
Documento de seguridad	X	X	X
Responsable de Seguridad		X	X
Funciones y obligaciones del personal	X	X	X
Registro de incidencias	X	X	X
Identificación y autentificación	X	X	X
Control de acceso	X	X	X
Control de acceso físico		X	X
Gestión de soportes	X	X	X
Copias de respaldo y recuperación	X	X	X
Auditoría periódica		X	X
Pruebas con datos reales		X	X
Distribución de soportes			X
Registro de acceso			X
Telecomunicaciones			X

Fuente: Agencia de Protección de Datos de la Comunidad de Madrid (2004:102).

7.5.3.1 El Documento de Seguridad

Existen siete requisitos exigidos por el Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007) a efectos de elaboración e implantación del Documento de Seguridad e incluso se adicionan 2 requisitos cuando se tratan de ficheros con medidas de seguridad de niveles medio y alto, que son los siguientes:

El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento (artículo 88 incisos 3 y 4 RD 1720/2007).

Lo primero a tener en cuenta a la hora de elaborar el Documento de Seguridad es que se trata de una obligación formal. El objeto del Reglamento de desarrollo de la LOPD es establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamientos, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos personales. Para poder implantar estas medidas, especialmente las organizativas, y que sean conocidas por las personas que intervengan en el tratamiento, es deseable que estén escritas y el Reglamento obliga a que estén, además recogidas en un Documento (Del Peso *et al.* 2004).

Todo responsable de ficheros que contengan datos personales deberá elaborar al menos un Documento de Seguridad, por tanto podrá corresponder esta labor tanto a empresarios, profesionales u órganos administrativos como a personas jurídicas, entendidas éstas últimas, a efectos de la LOPD, como unidades independientes sin perjuicio de su pertenencia a un grupo.

Asimismo, parece lógico llegar a un punto intermedio en el que se cree un Documento de Seguridad que contenga una parte general y común para la totalidad de los ficheros y que posteriormente se vaya desgajando en la información específica para cada nivel y cada fichero, especialmente relativa a la estructura de los mismos.

Las medidas de seguridad previstas para los ficheros con datos relativos a la salud de los pacientes, que se traten de forma automatizada, son las resumidas a continuación, cuya efectiva adopción deberá quedar reflejada a través de la elaboración e implantación del denominado Documento de Seguridad.

El Documento de Seguridad deberá contener como mínimo los siguientes aspectos:

a) Ámbito de aplicación.

b) Medidas, normas y procedimientos de seguridad.

c) Funciones y obligaciones del personal.

d) Estructura de los ficheros.

e) Procedimiento de incidencias y su registro.

f) Procedimientos de copias de respaldo y de recuperación de los datos.

g) Gestión y distribución de soportes.

h) Identificación y autenticación de los usuarios y registro de acceso.

i) Responsable de seguridad.

j) Controles de verificación.

k) Auditoría.

l) Control de acceso físico.

m) Transmisión telemática de datos.

El Documento de Seguridad deberá expresar el ámbito de aplicación del mismo, con especificación detallada de los siguientes extremos:

— Indicación del centro sanitario al que se aplica el documento de seguridad.

— Identificación del responsable del fichero y de la ubicación física del mismo.

— Relación de las personas a las que por tener acceso a los datos les sea de aplicación las medidas de seguridad establecida en el documento.

El Documento de Seguridad incluirá el conjunto de medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad aplicable. Se describirá detalladamente el sistema informático a través del cual se accede a los ficheros de datos, indicando los equipos informáticos existentes, aislados o conectados en red, características técnicas, la existencia de conexiones remotas y el tipo de las mismas (módem analógico, ADSL, RDSI, cable, etc.), el sistema operativo utilizado, los sistemas de protección existentes como antivirus o cortafuegos (firewalls) y las características técnicas de los mismos.

Se expresarán las medidas de seguridad existentes, tanto las medidas de seguridad físicas del local en el que se ubiquen los ficheros como las medidas de seguridad con que cuente el sistema informático.

El Documento de Seguridad, en relación al personal, debe relacionar todas y cada una de las personas que tengan acceso a los ficheros que contengan datos de salud de los pacientes, con indicación de las funciones, obligaciones y prerrogativas de acceso de cada uno de ellos

respecto a dichos datos. Igualmente se referirán a las personas físicas o entidades ajenas al centro sanitario que tengan acceso a tales datos por razón de servicios que presten a la organización (por ejemplo, empresas de mantenimiento de hardware o del software).

El Documento de Seguridad deberá expresar la estructura de los ficheros de los sistemas de información que los tratan. Se explicará la estructura de los ficheros que contienen los datos de salud de los pacientes, sus características, y en su caso, la finalidad de los mismos, aparte de la propiamente asistencial. Se describirán los programas informáticos utilizados para el tratamiento de los datos (APDCM, 2008).

El Documento de Seguridad establecerá un procedimiento de notificación, gestión y respuesta ante las incidencias que se puedan producir, implantándose un registro de incidencias.

El Documento de Seguridad contemplará un procedimiento de copias de respaldo y de recuperación de datos. Se expresará el procedimiento para la realización de las copias de seguridad, así como el procedimiento para la recuperación de datos, tales procedimientos deberán garantizar la reconstrucción de los datos de salud de los pacientes en el estado en que se encontraban al tiempo de su pérdida o destrucción. Se indicará la periodicidad con que se realicen las copias de respaldo, que deberá ser al menos de una copia por semana. Debe conservarse una copia de respaldo y del procedimiento de recuperación de los datos en un lugar diferente de aquel en que se encuentran los equipos informáticos en los que están almacenados los datos de salud.

El Documento de Seguridad debe contener un inventario exhaustivo de los soportes informáticos existentes que contengan datos de salud de los pacientes. Cuando un soporte informático que contenga datos de salud vaya a ser reutilizado o desechado, deberán adoptarse las medidas necesarias para evitar una posterior recuperación de la información contenida en el mismo, y además darle de baja en el inventario de soportes incorporado al documento de seguridad. Debe existir un registro de entrada de soportes informáticos y un registro de salida de los mismos (APDCM, 2008).

La distribución de soportes informáticos que contengan datos de carácter personal relativos a la salud de los pacientes, debe hacerse cifrando tales datos, o bien utilizando cualquier otro procedimiento

que garantice que los datos no puedan ser leídos ni manipulados durante su transporte.

El Documento de Seguridad recogerá una relación actualizada de usuarios con derecho de acceso al sistema de información que contenga los datos de salud de los pacientes. A estos efectos el centro sanitario, responsable del fichero, deberá establecer un sistema que permita la identificación inequívoca y personalizada de todo usuario que accede al sistema de información, así como la verificación de que dicho usuario está autorizado para acceder al sistema.

El Documento de Seguridad incorporará un registro de accesos, cuyo contenido deberá conservarse al menos durante dos años y ser verificado mensualmente por el responsable de seguridad.

El responsable del fichero debe designar a una o varias personas como responsables de seguridad, cuyo cometido será controlar y coordinar el cumplimiento de las medidas de seguridad implantadas en el documento de seguridad.

Al menos cada dos años ha de hacerse una auditoría interna o externa de los sistemas de información que contienen los datos personales relativos a la salud de los pacientes, así como el grado de cumplimiento de las medidas de seguridad de aplicación.

Únicamente el personal autorizado en el Documento de Seguridad deberá tener acceso a los locales donde se ubiquen físicamente los ficheros de datos de salud de los pacientes, debiendo establecerse un sistema de control de accesos a tales efectos (APDCM, 2008).

Si se transmiten datos de salud por medio de redes de telecomunicaciones debe procederse al cifrado de tales datos, o bien utilizar cualquier otro procedimiento que garantice que los datos no pueden ser leídos o manipulados por terceros.

A la vista de las medidas de seguridad expuestas, el problema reside en que el propio Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007) no distingue qué medidas se pueden considerar técnicas y cuáles organizativas, es a estos efectos que la extinta Agencia de Protección de Datos de la Comunidad de Madrid tenía publicado un manual de sesiones informativas, en el que efectúa lo que denomina una posible clasificación de los tipos de medidas, reconociendo algunas encuadran en los dos grupos, atendiendo a sus diferentes interpretaciones.

Según la Agencia de Protección de Datos de la Comunidad de Madrid, podría considerarse como medidas técnicas:

— Control de acceso (lógico).

— Identificación y autenticación.

— Notificación y gestión de incidencias.

— Gestión de soportes.

— Copias de respaldo y recuperación.

— Telecomunicaciones.

— Auditoría.

Conforme a la misma clasificación, serían medidas organizativas:

— Documento de seguridad.

— Funciones y obligaciones del personal.

— Responsable de seguridad.

— Notificación y gestión de incidencias.

— Control de acceso (físico).

— Distribución de soportes.

— Auditoría.

7.5.3.2 Las distintas figuras que aparecen en el Documento de Seguridad

El derecho fundamental a la protección de datos de carácter personal dota a la persona de una serie de facultades que son llevadas a la práctica mediante el ejercicio de los derechos de los que es titular. Pero todo derecho requiere la existencia de otra persona u otro organismo que pueda atender la conducta de obligado cumplimiento reclamada, para lo que la LOPD define la figura del *responsable del fichero*, y es ahí donde empieza una serie de responsabilidades que vamos a tratar.

La LOPD define en su artículo 3.d) al responsable del fichero o tratamiento como «la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento». El responsable del fichero debe es-

tar identificado en el impreso de creación, modificación y supresión de ficheros que se envía a la Agencia de Protección de Datos para ser inscritos en el Registro General de Protección de Datos.

El responsable del fichero estará sujeto al régimen sancionador establecido en el LOPD, y a lo largo de la propia ley y del Reglamento de desarrollo de la LOPD se establecen una serie de obligaciones para el mismo. Cuando el responsable del fichero realice tratamientos con ficheros calificados como de nivel medio o alto designará a una o varias personas para coordinar y controlar las medidas definidas en el Documento de Seguridad.

Esta figura se denomina *responsable de seguridad* y deberá estar identificado en el Documento de Seguridad obligatoriamente (artículo 95 del R.D. 1720/2007). En ningún caso esta designación supondrá una delegación de responsabilidad por parte del responsable del fichero. A lo largo de varios artículos del Reglamento de desarrollo de la LOPD están recogidas las funciones del responsable de seguridad.

Junto al responsable del fichero, también estará sujeto al régimen sancionador de la LOPD el *encargado del tratamiento*, definido en el artículo 5.i) del Reglamento de desarrollo de la LOPD como la «persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.».

La antigua LORTAD (Ley Orgánica 5/1992 de 29 de Octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal) no definía la figura del encargado del tratamiento como tal. El problema que se plantea con respecto al encargado del tratamiento es relativo a la aplicación del Reglamento de desarrollo de la LOPD, puesto que, aparentemente está a salvo de la obligatoriedad por parte del mismo de implantar las medidas de seguridad que corresponden al tipo de fichero tratado de acuerdo con el artículo 12 de la LOPD, da lugar a dudas en cuanto a la obligación de elaborar el Documento de Seguridad o de someterse a la auditoría bienal (APDCM, 2008).

Del Peso *et al.* (2004:60) señala que «de esta forma se empieza a establecer un entramado de responsabilidades que si en grandes entidades es cercenado a este nivel puede no ser suficiente, puesto que la responsabilidad a nivel interno de qué o no puede hacerse con los datos personales tendrá que partir de la persona que realmente asuma esas decisiones de forma delegada a nivel de su propio servicio, unidad o departamento».

7.5.3.3 Información facultativa en el Documento de Seguridad

A la hora de elaborar el Documento de Seguridad muchas veces el primer impulso será cumplir con el contenido exigido expresamente por el Reglamento de desarrollo de la LOPD, con cuya implantación conseguiríamos garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos personales.

Pero se debe ir más allá y considerar que el Documento de Seguridad es revisado, por ejemplo, por un alto directivo (un Gerente Director de un hospital o un Director del Centro sanitario) podría no tener ese mínimo conocimiento que se puede suplir fácilmente con una introducción.

Iniciados con el contenido del Documento de Seguridad y por la importancia que tiene de cara a la instrumentación de toda la normativa, resulta útil la identificación del responsable del fichero, el encargado del tratamiento y del o de los responsables de seguridad.

Es también de utilidad que el responsable del fichero señale si existe un encargado de tratamiento de los ficheros en el Documento de Seguridad, incluyendo un apartado en el que se detallen los datos del encargado del tratamiento indicando el tipo de servicio prestado y si es posible, incluyendo una fotocopia del contrato o al menos de la cláusula del mismo destinada a cumplir la obligación contenida en el artículo 12 de la LOPD e incluida en muchos contratos como cláusula de confidencialidad (APDCM, 2008).

Esta recomendación adquiere mayor valor a partir del momento en que la Agencia Española de Protección de datos admite que en las

inscripciones de ficheros en su Registro General figure un único encargado del tratamiento, recomendando que sea aquel que realice el tratamiento de datos que pueda implicar una mayor duración en el tiempo o riesgos mayores según el tipo y la cantidad de datos tratados.

7.5.3.4 Aplicación del Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de salud en centros sanitarios

La posición de Hernández Martínez-Campello (2004:219) señala «que la LOPD en su artículo 8, viene a establecer que la misma no es aplicable al tratamiento que los médicos efectúan a los datos relativos a la salud de sus pacientes, sino que en esta materia regirá la legislación estatal o autonómica sobre sanidad».

El legislador, con la ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, ha cumplido con la previsión contenida en dicho artículo 8 de la LOPD, en lo que se refiere a la legislación estatal sobre sanidad, puesto que la legislación autonómica ya existía anteriormente en determinadas Comunidades Autónomas como Cataluña, País Vasco, Navarra, Galicia, entre otras. Entre las leyes autonómicas, tanto la Ley Catalana 21/2000 como la Ley Foral Navarra 11/2002, disponen con similar redacción «que los centros sanitarios han de adoptar las medidas técnicas y organizativas adecuadas para proteger los datos personales recogidos y evitar la destrucción o la pérdida accidental y también el acceso, la alteración, la comunicación o cualquier otro procedimiento que no esté autorizado».

Es precisamente la Ley 41/2002, que entró en vigor el 15 de mayo de 2003, donde regula a nivel estatal lo que ya se recogía en las anteriores leyes autonómicas, esto es, que en el tratamiento que los médicos efectúan de los datos relativos a la salud, las medidas de seguridad a adoptar no son las reguladas por el Reglamento de desarrollo de la LOPD. El artículo 14.4 de la Ley 41/2002, establece lo siguiente: «Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar así su destrucción o su pérdida accidental».

Con tal disposición es evidente que lo que el legislador ha establecido es que sean las Comunidades Autónomas las que regulen cuáles han de ser las medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos de salud de los pacientes contenidos en las historias clínicas. Por lo tanto, la competencia para regular tal materia del tratamiento de los datos clínicos de los servicios sanitarios correspondería a las Comunidades Autónomas, no a una norma reglamentaria de ámbito estatal.

En este sentido, el artículo 17.6 de la Ley 41/2002 viene a confirmar lo expuesto «son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal».

No hace ninguna referencia a las medidas organizativas tratadas en el Reglamento de desarrollo de la LOPD, lo cierto es que la LOPD no determina concretas medidas técnicas de seguridad, sino que se limita a imponer la obligatoriedad de adoptar medidas de seguridad por parte del responsable del fichero, y, en su caso, del encargado del tratamiento, y difiere a su posterior desarrollo reglamentario su determinación. En definitiva sostiene Hernández Martínez-Campello (2004:219), conforme a la LOPD, la regulación del tratamiento, por parte de los profesionales sanitarios, de los datos relativos a la salud de sus pacientes se remite a la específica legislación sobre sanidad, la cual prevé para los servicios sanitarios la adopción de sus propias medidas de seguridad, ajenas a la regulación en el Real Decreto 1720/2007.

7.5.4 LA FIRMA ELECTRÓNICA

Si la firma autógrafa es el nombre, apellido o título que una persona escribe de su propia mano en un documento para darle autenticidad o para expresar que aprueba su contenido, la firma electrónica será de igual forma una identificación electrónica que se pondrá en forma electrónica por una persona, sobre un documento electrónico para darle autenticidad o para expresar que aprueba su contenido.

No es necesario acudir a definiciones complejas pues se debe buscar, en un principio, asociar los conceptos en los que solamente cambiará el elemento, bien del soporte –papel o electrónico–, o bien de la representación gráfica de la identificación del firmante, en un escrito sobre un papel o en un escrito sobre soporte electrónico (Davara Rodríguez, 2005).

La Cámara de Comercio Internacional señala que debe entenderse por firma electrónica: «Toda transformación de un mensaje mediante la utilización de un criptosistema asimétrico de modo que una persona en posesión del mensaje firmado y de la clave pública del firmante puedan determinar con exactitud: a) si la transformación fue producida mediante la utilización de la clave privada que se corresponde con la clave pública del firmante y b) si el mensaje firmado ha sido alterado desde que se produjo la transformación».

La Ley 59/2003 de España sobre firma Electrónica, de 19 de diciembre la define en el artículo 3 la define como «el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante».

Asimismo, la Ley 59/2003 define a la firma electrónica avanzada como: «la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control».

Se considera firma electrónica reconocida «la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma».

La Directiva 1999/93/CE la define como: «los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación».

La Ley 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación de fecha 8 de agosto de 2011 en el numeral 5 del parágrafo IV del artículo 6 define así a la firma digital: «es la firma electrónica que identifica únicamente a su titular creada por métodos que se encuentran bajo el absoluto y exclusivo control de su titular, susceptible de verificación y está vinculada a los datos del do-

cumento digital de modo tal que cualquier modificación de los mismos ponga en evidencia su alteración».

El Decreto Supremo 1793 Reglamento a la Ley 164 para el desarrollo de Tecnologías de Información y Comunicación de fecha 13 de noviembre de 2013 define, en el inciso d) de parágrafo III del artículo 3, que la firma electrónica: «es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carece de alguno de los requisitos legales para ser considerada firma digital».

Por último la Ley UNCITRAL indica que firma electrónica consiste en: «los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos».

De estas definiciones prácticamente solo se encuentra una total igualdad en el reconocimiento de la firma electrónica como datos en forma electrónica, consignados o asociados a otros datos electrónicos y que sirven para identificar al que firma. Se trata, al igual que la firma manuscrita, de un instrumento cierto de atribución de paternidad a una declaración de voluntad. Por medio del mismo se conoce la persona que emite la declaración y se establece con positiva certeza que la declaración emitida corresponde a la voluntad o conocimiento declarado del remitente (García Más, 2004).

7.5.4.1 **La criptografía**

La criptografía comprende la transformación, ocultación de la información, convirtiendo el mensaje en ininteligible (cifrado) aparentemente y el procedimiento a la inversa transformando el mensaje en inteligible (descifrado) para aquellos destinatarios deseados. Dicho de otra manera, «es un conjunto de técnicas que permiten cifrar y descifrar información».

Criptografía (Cripto = secreto y Grafía = escritura). Métodos documentados desde Julio César, siglo I antes de Cristo. La criptografía es una técnica clásica que se ha utilizado desde tiempos inmemoriales,

no obstante, el origen de la criptografía moderna se puede fijar durante el período de la Segunda Guerra Mundial donde se utilizaba para enviar mensajes con la finalidad de que el enemigo no pudiera acceder a información sensible; el propósito era esencialmente militar.

En la actualidad, la criptografía está considerada como una Tecnología de Doble Uso, en el sentido de que puede ser utilizada con la finalidad civil y militar, es por este motivo que existen restricciones y hasta prohibiciones para su exportación a países considerados peligrosos. En Francia existía una legislación muy restrictiva en el uso de la criptografía sin permitir a los poderes públicos luchar eficazmente contra actuaciones criminales, orientación que ha sido cambiada encaminándose hacia una libertad total en el uso de aquella.

Primera aproximación de criptografía: Ciencia que estudia los principios, métodos y medios de ocultar el significado de un mensaje, es decir, de garantizar su confidencialidad. En el presente estudia los principios, métodos y medios de transformar los datos para ocultar información contenida en ellos, garantizar su identidad, autenticidad y prevenir su repudio.

El criptoanálisis es la materia contraria, investiga métodos de descubrir informaciones cifradas sin el conocimiento de la información secreta. El estudio de ambas criptografía y criptoanálisis constituye el objetivo de la rama del saber denominada «criptología».

Los mecanismos que se utilizan para cifrar y descifrar serán las llamadas claves, que se asimilan a números de gran longitud para que sean seguras y que siguen un algoritmo matemático. Las mencionadas claves pueden ser generadas por un sistema informático del usuario, o bien por un sistema central que las transportará, más tarde, al sistema del usuario en forma segura; en este segundo caso, una vez creadas y transportadas serán destruidas.

Básicamente, se utilizan dos técnicas para encriptar y desencriptar. De modo que se distingue básicamente entre la denominada técnica de cifrado simétrico, también conocida como cifrado en clave convencional, secreta, privada, criptografía de clave simétrica, y por otro lado la técnica de cifrado asimétrico, identificada también como de clave pública, criptografía de clave asimétrica.

La primera de ellas es una técnica sencilla donde tanto emisor como receptor del mensaje del mensaje comparten una única clave que permitirá cifrar y descifrar la información.

El algoritmo de clave simétrico más utilizado es conocido como DES, *Data Encrytion Standard*, estándar de cifrado de datos, que tiene como finalidad proporcionar confidencialidad en las comunicaciones.

La criptografía de clave simétrica presenta ventajas e inconvenientes, entre las primeras destacan la sencillez de su utilización, así como, la rapidez de los algoritmos utilizados. Los inconvenientes se vinculan a que la clave que es compartida por el emisor y el receptor, se mantengan en secreto, lo que comporta la utilización de medios seguros para su transmisión, de lo contrario terceras personas podrían acceder al contenido de los mensajes. Por ejemplo, si se envía la clave privada utilizando correo electrónico, no es un medio seguro ya que un tercero puede captarla durante la transmisión. Ni tan siquiera es recomendable utilizar como medio de transmisión el tradicional servicio de correos, o la línea telefónica, siendo la entrega en mano el método más eficaz para evitar que la clave sea descubierta durante la transmisión, pero insuficiente cuando las partes se encuentren geográficamente separadas, realidad frecuente en el comercio electrónico.

La técnica de cifrado asimétrico es más complicada que la anterior, consiste en la utilización de una par de claves (clave privada y clave pública) para cada uno de los interlocutores (emisor y receptor), asociadas matemáticamente de forma que lo que se cifra con una, solo puede ser descifrado con su pareja y viceversa. El cifrado asimétrico, se utiliza para conseguir una comunicación cifrada como para el proceso de firma electrónica.

Por lo tanto intervienen dos claves, por un lado la clave privada que tiene finalidad doble, en función de si es utilizada en el ámbito del cifrado, o en el de la firma electrónica. En el primero, en el cifrado, es usada para descifrar la información recibida y en el segundo, firma electrónica, es indispensable para su creación. En todo caso, es fundamental que la clave privada se mantenga en secreto por lo que es aconsejable que esté bien guardada, ya sea en el ordenador, ya sea en una tarjeta inteligente de uso personal y si se desea todavía mayor seguridad, accediendo a ella mediante un número de identificación personal, o incluso utilizando sistemas de identificación biométricos

como pueden ser el reconocimiento de la voz, la huella digital (De Quinto Zumárraga, 2004).

Por otro lado, la clave privada sirve para poder cifrar la información en el ámbito del cifrado y para verificar la firma en el campo de la firma electrónica. A diferencia de lo que ocurre con la clave privada, la pública ha de ser ampliamente conocida por todos y fácilmente accesible.

Ambas claves se encuentran relacionadas entre sí por operaciones matemáticas. Al inicio se trata de simples operaciones aritméticas (generalmente operando con números primos), más tarde se recurrió a operaciones algebraicas más complicadas y en la actualidad se emplean técnicas de encriptación o cifrado que utilizan un sistema de curvas elípticas. El algoritmo de clave asimétrica más conocido es RSA (Rivest, Shamir y Adleman).

Con el conocimiento de una de las claves es imposible deducir la otra clave asociada como tampoco es posible que exista un par de claves iguales, debido a que el par de claves ha de ser único de cada persona o entidad. En caso contrario, se crearía confusión sobre la autoría de los mensajes, comprendiendo la confidencialidad. Por último, es necesario que el proceso de generación de claves sea fiable y seguro.

La ventaja esencial vinculada a la utilización de esta técnica estriba en que no sea necesaria la distribución de la clave en un canal inseguro como es Internet. El principal inconveniente que presenta es que la clave pública que utilizamos para cifrar una información pertenezca efectivamente a su titular y no a un impostor que usurpa su personalidad.

7.5.4.2 **Sellamiento electrónico: funciones HASH**

Para la prueba de integridad e individualización del documento, para evitar la duplicación o su confusión con otro de la misma fecha y contenido, se emplean los «sellos o sellamiento electrónico» o funciones *Hash* conjuntamente con la firma electrónica.

Así también, debido a que la aplicación de criptografía asimétrica sobre la totalidad del mensaje puede resultar costosa, especialmente si éste es muy extenso, se aplica sobre el mensaje inicial el algoritmo

o función *hash*, y se obtiene un resumen del mismo (denominado compendio del mensaje o huella digital), caracterizado por su irreversibilidad (esto es, a partir del resumen no puede obtenerse el mensaje completo inicial) y por ser único del mensaje (es decir, computacionalmente imposible obtener un segundo mensaje que produzca el mismo resumen *hash*), de forma que cualquier cambio en el mensaje produciría un resumen o *hash* diferente.

En conjunto, las funciones *Hash*, Sellamientos Electrónicos, Firma Electrónica, Centros de Compensación, Acuerdos de Intercambio forman la base de la firma y contratación electrónica.

El sellamiento introduce la fecha y la hora de la transacción que queda integrada en el documento que será firmado junto con su contenido con la clave privada del remitente. Se trata de una condensación algorítmica del mensaje o contrato completo, que se incluye en el mismo mensaje y que se procesa éste cada vez que se transmite el documento, así se puede comparar si coincide con el sello original.

Las funciones de *hash* consisten en sistemas que, partiendo de todos los datos del documento, calculan un compendio codificado (*digest*) que se firmaría electrónicamente con la operativa antes indicada, formando así la firma electrónica. Posteriormente el destinatario recuperará, con la clave pública del remitente, el resumen *hash* recibido de la firma del documento y lo comprobará con el *hash* que le resulte del documento recibido y si ha variado es que ha perdido la integridad, y/o la autoría del documento recibido, en cambio si coincide, no cabría duda de la integridad del documento (Vázquez Iruzubieta, 2002).

Las características fundamentales de la función *hash* estriban en su carácter único, dado que no pueden existir dos mensajes diferentes con el mismo resumen, siendo detectable por tanto cualquier alteración, es irreversible, ya que no se puede obtener el texto completo a partir del resumen.

7.5.4.3 **Problemas relativos a la seguridad**

La actual deficiente seguridad en la transmisión de información a través de Internet hace necesario el establecimiento y cumplimiento de unos objetivos concretos que permitan paliar este problema, a los

que se les identifica como autenticación, integridad, no repudio y confidencialidad.

— *La autenticación:* Permite asegurar que quién envía la información es realmente quien dice ser y no un tercero. Por ejemplo, A recibe un mensaje de B y quiere estar seguro que es B quién lo envía y no otra persona. Los problemas se pueden plantear cuando alguien suple la identidad de una persona o empresa.

— *La integridad:* supone tener la certeza de que el mensaje no ha sido manipulado ilícitamente durante la transmisión, o como mínimo si se ha manipulado tener conocimiento de ello. Es importante conocer si un mensaje ha sido alterado ya que, en caso contrario, pueden cambiar, suprimir las manifestaciones realizadas e incluso atribuir unas nuevas. Para evitar la manipulación de los mensajes, se acudirá de nuevo a una solución técnica como es la firma electrónica, que mediante la aplicación de una determinada función con unos caracteres específicos, permite averiguar cualquier cambio que se haya producido en la información transmitida.

— *El no repudio:* se vincula con la obtención de seguridad, en el sentido de que no se pueda negar la participación de los intervinientes en una comunicación electrónica. Bajo este concepto, se puede diferenciar dos acepciones: no repudio de origen, que implica que el emisor del mensaje no niegue a posteriori haberlo enviado y no repudio de destino, que conlleva que el receptor no niegue más tarde la recepción del mensaje. En definitiva se protege a las partes de la comunicación frente a la negación de que dicha comunicación haya tenido lugar. Para tener prueba de la transmisión se recurrirá a la firma electrónica avanzada, que permite la vinculación de una persona concreta a un texto determinado mediante un sistema de claves. Como se puede observar el no repudio se encuentra íntimamente ligado a la autenticación.

— *La confidencialidad:* se asocia a la seguridad de que la información enviada a través de la red sólo puede ser conocida por su destinatario, de forma que resulte infructuoso para terceros el conocimiento de aquélla en caso de interceptación ya sea accidental o voluntariamente. Para conseguirla en las comunicacio-

nes electrónicas se acudirá por lo general a soluciones técnicas basada en la criptografía.

7.5.4.4 Prestadores de servicios de certificación

El artículo 2.2 de la Ley 59/2003, de firma electrónica de España, define al prestador de servicios de certificación como «la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica».

La Ley 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación de fecha 8 de agosto de 2011 de Bolivia establece en el artículo 82 a la Entidad Certificadora: «Pueden constituirse y operar como entidades certificadoras, las personas jurídicas de derecho público o privado en la prestación de servicios de certificación digital, las que deben cumplir con los requisitos técnicos, económicos y legales establecidos en la presente Ley y su reglamento».

El primero de los requisitos exigidos para que la firma electrónica avanzada alcance la superior modalidad de firma electrónica reconocida radica en estar basada en un certificado reconocido. Ello pone en evidencia, que ni la técnica más sofisticada de firma electrónica ha conseguido el objetivo anhelado de asegurar la identificación del autor del mensaje, pues aunque el certificado reconocido integre en la firma electrónica reconocida como uno de sus elementos, lo cierto es que la técnica no ha podido funcionar por sí misma, que la máquina ha llamado en su auxilio al hombre, a fin de cuentas, quien garantiza que la clave pública pertenece a una persona determinada no es la firma electrónica en sí, sino el prestador de servicios de certificación por medio de un certificado digital incorporado a la firma (Rodríguez Adrados, 2004).

La sociedad de la información necesita para funcionar una gran variedad de servicios de intermediación a los que se refiere la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), de 11 de julio de España, en sus artículos 13 y siguientes: operadores de redes; proveedores de acceso; prestadores de servicios de copia temporal de datos, de alojamiento o almacenamiento de datos, de búsqueda de contenidos, etc., y muy especialmente de prestadores de servicios de certificación, que son los

sujetos que hacen posible el empleo de la firma electrónica, los que van a suplir sus deficiencias.

Estos prestadores de servicios de certificación han de ser terceros de confianza de las partes *(Trusted Third Party)* y su misión primaria es la de certificar que determinada clave pública pertenece a una persona y que se encuentra vigente y podrán para ello generar, distribuir y controlar las parejas de claves, sin almacenar ni copiar la privada que es secreta, así como garantizar facultades de representación y cualquier otro atributo o circunstancia del expedidor del mensaje que se considere de relevancia jurídica para la validez del contrato informático a realizar.

7.5.4.5 **Los certificados electrónicos**

Los prestadores de servicios de certificación tienen como principal misión la expedición de certificados. La Ley 59/2003 define en el artículo 6.1 el certificado electrónico «un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad», esto es, que vincula una clave pública a un firmante determinado y confirma la identidad de éste, aunque lo que en realidad puede confirmar no es la identidad del firmante sino la identidad del titular de dicha clave pública.

El artículo 6.2 de la Ley 59/2003 formula el concepto de firmante como «la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa». Se trata pues de un documento, aunque de hecho se integre con los datos de creación de firma –con la clave privada– para encriptar los mensajes, y por ellos mismo es necesariamente un documento electrónico, nunca podría ser un documento en papel (Rodríguez Adrados, 2004).

El inciso *g)* del artículo 6 del Decreto Supremo 1793 Reglamento de la Ley 164 para el desarrollo de Tecnologías de Información y Comunicación formula el concepto de signatario «es el titular de una firma digital que utiliza la misma bajo su exclusivo control y el respaldo de un certificado digital proporcionado por entidades certificadoras autorizadas».

La categoría más elevada de estos certificados electrónicos son los certificados reconocidos, aquellos otros certificados que no reúnan todos sus requisitos pueden llamarse certificados simples. El certificado se habrá de solicitar al prestador de servicios de certificación de su elección. Aunque existen certificados para una operación concreta, en la práctica suelen expedirse para todas las operaciones de determinada especie que el solicitante pueda realizar durante un período de tiempo determinado, que en el caso de los certificados reconocidos no puede ser superior a cinco años (artículo 8.2 Ley 59/2003, redactado por la disposición final sexta de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones).

La vigencia de los certificados, en consecuencia, se extingue, según el artículo 8 de la citada ley, por expiración de su período de validez, y también por su revocación, fallecimiento o incapacidad sobrevenida del firmante, resolución judicial o administrativa, cese en la actividad del prestador de servicios de certificación, y por cualquier otra causa lícita prevista en la declaración de prácticas de certificación. Los prestadores de servicios de certificación suspenderán la vigencia de los certificados por solicitud del firmante o cualquier otra causa lícita prevista en dicha declaración de prácticas. Y tendrá lugar la extinción, o la suspensión por existencia de dudas fundadas al respecto en los casos de violación o puesta en peligro del secreto de la clave privada y la alteración de los datos aportados para la obtención del certificado (artículos 8 y 9 de la Ley 59/2003).

La Ley 164 General de Telecomunicaciones, Tecnología de Información y Comunicación en el numeral 1 del parágrafo IV del artículo 6 define así al Certificado Digital: «es un documento digital firmado digitalmente por una entidad certificadora autorizada que vincula unos datos de verificación de firma a un signatario y confirma su identidad. El certificado digital es válido únicamente dentro del período de vigencia, indicado en el certificado digital».

El artículo 24 del Decreto Reglamentario de la Ley 164 para el desarrollo de Tecnologías de Información y Comunicación establece que los certificados digitales deben ser emitidos por una entidad certificadora autorizada, responder a formatos y estándares reconocidos internacionalmente y fijados por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), contener como mínimo los datos que permitan identificar a su titular, a la entidad

certificadora que lo emitió, su periodo de vigencia y contemplar la información necesaria para la verificación de la firma digital.

Un certificado digital puede ser revocado por la entidad certificadora en los siguientes casos: *a)* A solicitud de su titular, *b)* Por fallecimiento del titular del certificado, *c)* Por disolución o quiebra de la persona jurídica titular del certificado, *d)* Por sentencia condenatoria ejecutoriada en contra del titular del certificado, *e)* Sentencia judicial que declare la ausencia o interdicción del titular del certificado, *f)* Por requerimiento de autoridad competente, *g)* Cuando se corrobore que el titular del certificado digital no ha custodiado adecuadamente los mecanismos de seguridad, *h)* De comprobarse por parte de la ATT que se han producido vulneraciones técnicas del sistema de seguridad de la entidad certificadora, *i)* Por incumplimiento de las causas pactadas entre la entidad certificadora con el titular del certificado digital (artículo 31 D.S. 1793).

7.5.4.6 **Utilización de la firma electrónica**

El uso de la firma electrónica no se encuentra limitado a sectores concretos ni a personas o entidades determinadas, pudiendo utilizarse tanto en el sector público como en el sector privado, bien por particulares, bien por empresas.

En el sector privado, su utilización puede estar vinculada a cuestiones relacionadas con la contratación privada por vía electrónica, entre empresa y consumidor (por ejemplo compraventa de bienes de consumo), entre empresa y empresa (por ejemplo pedido a un suministrador) o incluso entre consumidores particulares (por ejemplo compraventa de una colección de sellos).

Por otra parte, la utilización de la firma electrónica en el sector público (incluye las relaciones entre administración y los entes públicos y entre aquella y los ciudadanos, respectivamente) puede estar relacionada con actuaciones tan habituales como la renovación de documentos oficiales (por ejemplo el Documento Nacional de Identidad-DNI); la solicitud de prestaciones sociales a los organismos competentes por medios electrónicos (por ejemplo prestación por incapacidad permanente); la remisión electrónica de documentos de la Seguridad Social; la presentación de documentos para ad-

juntar a un expediente administrativo abierto; las declaraciones de impuestos, etc.

La diferencia de uso en uno u otro sector radica en que en el sector público su utilización puede quedar supeditada al cumplimiento de unas condiciones adicionales establecidas por norma que en todo deberán ser objetivas, razonables y no discriminatorias y en ningún caso obstaculizarán la prestación de servicios al ciudadano cuando intervengan diferentes administraciones públicas nacionales o extranjeras (Rodríguez Adrados, 2004).

El Sistema de Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS) del Ministerio de Sanidad, Servicios Sociales e Igualdad (MSPS) de España tiene como estrategia de seguridad alguna medida de control previo al acceso, más allá de los que las normas mencionadas exigen (firma electrónica reconocida y adscripción de los profesionales a grupos distintos).

El ciudadano tiene acceso a todos y cada uno de los informes que conforman su HCDSNS, que se encuentran custodiados en cada una de las Comunidades Autónomas en que se han generado. Todo ciudadano incluido en el registro de usuarios (Base de datos de TSI de su Comunidad) y que se haya dotado de firma electrónica reconocida (o DNI electrónico) podrá acceder a los documentos electrónicos que estén disponibles, a través de la web habilitada por su Servicio de Salud, imprimirlos o descargarlos en un dispositivo de almacenamiento local.

Adicionalmente a los requisitos de seguridad impuestos por la legislación vigente, y dado el carácter de la información a manejar, los servicios del Sistema Nacional de Salud dispondrán de mecanismos de seguridad, que mediante el uso de técnicas de criptografía y clave pública garanticen:

— La identidad de las personas previamente autorizadas.

— La autenticidad de los agentes que dicen actuar en su nombre.

— La garantía de no repudio, evitando el no reconocimiento por parte de los agentes de la realización de una operación en el sistema.

— La privacidad de la información objeto del intercambio, de forma que ésta no sea revelada a terceros de ninguna forma, ni intencionada ni accidental.

— La integridad de la información, garantizando que ésta no ha sido manipulada en ningún punto de la comunicación ni intencionada ni accidentalmente.

La aplicación web diseñada por el Ministerio de Sanidad, Servicios Sociales e Igualdad (MSPS) para facilitar el acceso de los usuarios del sistema de HCDSNS a las funcionalidades, dispone de dos presentaciones diferentes:

— *Acceso para profesionales:* Cada Comunidad Autónoma puede integrarla en la Intranet sanitaria de su Servicio de Salud.

— *Acceso para ciudadanos:* El acceso ha de realizarse a través de la página web del Servicio de Salud en el que cada ciudadano se encuentre dado de alta en tarjeta sanitaria.

En ambos casos, el acceso del usuario es concedido tras la comprobación de la identidad de quien intenta acceder (autenticación) y su pertenencia al registro de usuarios, profesionales y ciudadanos, legitimados para hacer uso del sistema (autorización). En ambos casos, la responsabilidad de garantizar que cada acceso al sistema cumple los requisitos necesarios recae en la Comunidad Autónoma a la que se encuentra vinculado el usuario del sistema, en calidad de profesional sanitario o ciudadano dado de alta en dicha Comunidad (MSPS, 2009).

7.5.5 LA AUDITORÍA INFORMÁTICA COMO HERRAMIENTA PARA LA PROTECCIÓN DE LA INFORMACIÓN

7.5.5.1 **La auditoría de la seguridad**

La auditoría de seguridad puede abarcar muchos aspectos, como puede ser el grado de protección de las instalaciones o de las personas, pero esta investigación se centrará en la seguridad relacionada con datos e información, y más concretamente en los datos de carácter personal, y por tanto en relación con la LOPD y sobre todo el Reglamento de desarrollo de la LOPD de España (Real Decreto 1720/2007).

Habría de distinguirse entre auditoría informática y auditoría de sistemas de información, aunque a veces se usen los términos de ma-

nera indistinta, en parte es una evolución, igual que el área funcional de las entidades, que inicialmente se pudo llamar Mecanización y luego Proceso de Datos, después se llamó Informática y luego en algunos casos Sistemas de Información, pero también es porque la mayor parte de los sistemas de información empresariales hoy día están soportados por tecnología (Del Peso Navarro, 2003).

Aguilera López (2010:22) indica que: «La auditoría es un análisis pormenorizado de un sistema de información que permite descubrir, identificar y corregir vulnerabilidades en los activos que lo componen y en los procesos que realizan. Su finalidad es verificar que se cumplen los objetivos de la política de seguridad de la organización. Proporciona una imagen real y actual del estado de seguridad de un sistema de información».

La denominación que se refiere a sistemas de información abarcaría todas las fases del ciclo de vida de los datos-información, incluyendo procesos manuales, así como el camino que siguen los resultados obtenidos en papel, y de este modo la auditoría no se limitaría a las plataformas tecnológicas, y dentro de la colaboración entre auditores informáticos y auditores financieros serían los sistemas de información el área común.

La norma ISO 7498-2 ya consideraba que Auditoría de la Seguridad era: «Una revisión y examen independientes de los registros y actividades de un sistema a fin de verificar si los controles del sistema son adecuados, para garantizar el cumplimiento con la política establecida y con los procedimientos operativos, para detectar problemas de seguridad, y para recomendar posibles cambios en la política de control y en los procedimientos».

Sobre la independencia de la auditoría cabe preguntarse si es más independiente la auditoría interna o la externa, puede decirse que ambas deben serlo. La interna mediante su dependencia jerárquica y la externa por que no tenga otro tipo de servicios o relaciones incompatibles con la entidad, y porque no pueda ofrecerle servicios complementarios, por ejemplo, paquetes para que mejore la situación que el proceso de auditoría ha evaluado y recomendado mejorar (Del Peso *et al.*, 2004).

También hay diferencias entre auditoría e inspección, y en el caso que ocupa a esta investigación está claro: la auditoría que exige el Reglamento de desarrollo de la Ley Orgánica 15/1999, frente a la

inspección que puede realizar una de las Agencias de Protección de Datos (estatal o autonómica).

7.5.5.2 **Control interno**

Se suele decir que la auditoría es la evolución del control interno, y como Sistema de Control Interno se puede considerar el conjunto de procesos, funciones, actividades, dispositivos, entre otros, cuya misión total o parcial sea garantizar que se alcanzan los objetivos de control, y que los sucesos no deseados se evitarán, o bien detectarán y se corregirán.

Señala Del Peso *et al.* (2004:66) que los objetivos de control se pueden definir como: «Declaraciones de cada entidad sobre el resultado final deseado o del propósito alcanzado mediante la implantación de procedimientos de control».

COSO *(The Committee of Sponsoring Organizations of the Tradeway Commission)* define el control interno como «un proceso, que lleva a cabo el Comité de Dirección, la Dirección u otro personal, diseñado para aportar garantía razonable acerca del cumplimiento de los objetivos dentro de las siguientes categorías:

— Eficacia y eficiencia de las operaciones,

— Fiabilidad de los informes financieros,

— Cumplimiento de la leyes y normas/regulaciones, que sean aplicables».

Y especifica COSO:

— El control interno es un proceso, y un medio relacionado con un fin, no un fin en sí mismo.

— El control interno lo llevan a cabo personas, y se trata no sólo de políticas escritas y de formularios, sino de personas a cada nivel de la entidad.

— Se espera que el control interno aporte sólo una garantía razonable, no una garantía absoluta, a la Dirección y al Comité o Consejo de la entidad.

— En el caso del Reglamento de desarrollo de la LOPD, se alude a la auditoría en su artículo 96, y hay otros aspectos que pueden considerarse como control interno.

En el artículo 88.4 dice que el Documento de Seguridad deberá contener «los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento…», y se recoge dentro de las medidas de nivel medio o nivel alto, y antes de hablar del responsable de seguridad, por lo que se entiende que puede ser por parte del responsable de seguridad o no.

En el artículo 95 se indica que «En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo».

Probablemente en entidades pequeñas el control lo lleven a cabo de forma directa y en otros se trate de coordinar las revisiones que otros realizan, pero se puede entender que son capas de control interno, y que la auditoría es una capa más, para evaluar el sistema de control interno.

7.5.5.3 **Perfil del auditor de seguridad**

El perfil de un auditor de seguridad de la información es el que corresponde a un Ingeniero e Ingeniero Técnico en Informática en cualquiera de sus especialidades, pero más concretamente la especialidad de Gestión o también a un profesional al que se le presupone cierta formación técnica en informática y experiencia en el sector, independencia y objetividad, madurez, capacidad de síntesis, análisis y seguridad en sí mismo.

No hay nada regulado al respecto, igual que ocurre en la consultoría, siendo el mercado el que va seleccionando. El certificado más prestigioso y más afín actualmente es el CISA *(Certified Information Systems Auditor)* de ISACA *(Information Systems Audit and Control Association/Foundation)*, cuyos exámenes se celebran cada año en varias ciudades españolas y en muchos países.

7.5.5.4 **Cómo se realiza una auditoría**

Para saber cómo se realiza una auditoría se recurre a lo establecido por Del Peso *et al.* (2004:71) que resume como se realiza la mis-

ma. Señala que han de quedar muy claros, y más aún en el caso de una auditoría externa:

— Objetivos.

— Alcance/ámbito.

— Profundidad.

— Período al que se refiere, que normalmente no es aplicable y se trata de evaluar la situación en el momento presente.

Para determinarlos o entenderlos y poder estimar el esfuerzo se han de conocer aspectos de la entidad como su complejidad y sus procesos no tanto tecnológicos sino de negocio, pero también sus centros, plataformas y recursos afectados por la revisión y evaluación.

En el caso de auditoría, el Reglamento de desarrollo de la LOPD se debe realizar solo de los ficheros obligatorios de nivel medio y alto. Pero a veces se requiere una revisión más completa, tal vez en dos informes diferenciados, e incluso de ficheros que no tengan datos personales. En ocasiones el cliente cree que tiene un único fichero afectado y en realidad tiene más por haber asignado mal el nivel. A veces es un fichero único, pero se trata de evaluar las medidas y nivel de cumplimiento del encargado del tratamiento, que está en otra ciudad, lo que debe saberse de antemano.

A partir de los puntos anteriores se estimará el esfuerzo/tiempo, los recursos necesarios y su perfil, así como el presupuesto, y se hará la planificación correspondiente e incluso el programa de trabajo, y en otras ocasiones sólo una planificación inicial, y la definitiva cuando se ha aprobado la asistencia.

En función del objetivo se determinarán las fuentes de información y de documentación más idóneas y las pruebas a realizar, en principio pruebas de cumplimiento y después posibles pruebas sustantivas, y también las funciones y personas a entrevistar, las posibles herramientas a utilizar y las técnicas a aplicar, entre otros, hasta llegar a alcanzar evidencias necesarias para poder evaluar la situación y las posibles debilidades o incumplimientos.

Generalmente se irán desarrollando productos parciales y se irá elaborando el borrador del informe a medida que se va avanzando en la auditoría. El borrador se discutirá con el cliente para aclarar los

diferentes puntos, y así llegar al informe definitivo, que en ocasiones tendrá el mismo contenido del borrador por no existir variaciones. En el caso de los internos suele haber, una vez determinadas las prioridades y el plan de acción, un seguimiento.

La evaluación se debe hacer contra algún patrón, que puede ser interno, como la normativa existente o el contrato de servicios entre entidades y sus anexos, o bien totalmente externo, como la norma ISO/IEC 27004, COBIT de ISACA, o cualquier estándar reconocido, y en todos los caos pueden haber interpretaciones o valoraciones diferentes, pero más difícil aún puede ser cuando no hay ningún patrón porque la entidad no tenga ningún tipo de norma y haya pedido una auditoría general de seguridad, habrá que advertirle que se puede hacer frente a estándares generalizados, que podrán equivaler a los principios generalmente aceptados que dicen los auditores de cuentas.

7.5.5.5 **Estándares**

Los procesos de auditoría se deben basar en estándares contrastados y aceptados, y a diferentes niveles, tanto respecto a cómo hacer el proceso de auditoría como modelos contra los que comparar situaciones.

En cuanto a estándares de cómo realizar la auditoría, ISACA *(Information Systems Audit. And Control Association/Foundation)* puede ser una de las mejores fuentes, además de lo que cada entidad pueda tener. Lo primero que recoge ISACA es el Código de Ética Profesional que deben cumplir sus miembros, además indica los principios de independencia, competencia, planificación del trabajo, la necesidad de alcanzar evidencias, el uso de técnicas y de muestreos, y elaboración de informes, resumiendo mucho (Del Peso *et al.*, 2004).

Están además, por parte de ISACA, los Objetivos de Control (COBIT) y las guías. Otros estándares son las propias normas ISO, especialmente la citada norma ISO/IEC27004.

7.5.5.6 **Auditoría del Reglamento de desarrollo de la Ley Orgánica 15/1999**

La Auditoría es obligatoria para los ficheros de nivel medio y alto, así como los ficheros y tratamientos no automatizados, según los ar-

tículos 96 y 110 del Reglamento de desarrollo de la LOPD, y puede ser deseable para ficheros de datos personales de nivel básico y para todo tipo de ficheros y de sistemas. Aunque en muchos encargos el cliente especifique que quiere la auditoría informática que exige el Real Decreto 1720/2007, la auditoría abarca muchos aspectos, y que en el Reglamento figura sin adjetivos.

El artículo 96 del Reglamento de desarrollo de la LOPD dice sobre auditoría:

1. «A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

2. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

3. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

4. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.»

Los sistemas de información pueden abarcar no sólo servidores, sino también terminales, que pueden ser móviles, y en todo caso las instalaciones pueden ser de un encargado del tratamiento, y a su vez éste tener contratados otros servicios, se entiende que con consentimiento del responsable del fichero, como puede ser la custodia de soportes o los procesos en caso de contingencia. En las auditorías de encargados de tratamiento se suele encontrar a los interlocutores pre-

ocupados por los resultados, suelen estar acostumbrados y saben que se les va a preguntar y menudo tienen toda la información preparada, lo que facilita la revisión.

Cabe resaltar que la auditoría se realizará al menos cada dos años, es decir bienal y no bianual que es dos veces al año, término que figura en escritos y webs de firmas de prestigio.

7.6 GESTIÓN DEL CAMBIO EN EL SECTOR SANITARIO

El término gestión del cambio se aplica a las acciones relacionadas con la puesta en práctica de planes de actuación que afectan la estructura, organización y funcionamiento de las organizaciones, a fin de conseguir los objetivos de mejora establecidos.

Ciertamente las instituciones tienen elementos propios que las diferencian, de forma que se puede decir que no existen dos organizaciones exactamente iguales, por ello, las situaciones de cambio, y de gestión del cambio, serán en principio distintas en cada caso. Este cuerpo de conocimientos de gestión del cambio está constituido por modelos, métodos, técnicas, herramientas, habilidades y otras formas de experiencia sistematizada. Su objeto básico es el estudio del comportamiento de organizaciones y de la manera de actuar sobre él. Los elementos que la constituyen se basan en la psicología, la sociología, la administración y gestión de empresas, la ingeniería de sistemas y la teoría de sistemas generales.

Monteagudo Peña (2004:501) señala que «la sanidad se encuentra en plena transformación como resultado de la evolución combinada de varios factores, entre los que destacan la implantación de nuevos modelos de organización y provisión de los servicios sanitarios y de las nuevas tecnologías de la información y comunicaciones. El cambio aparece como una constante, y además se está produciendo con carácter drástico más que incremental, por lo que la gestión del cambio se ha convertido en una tarea esencial para los directivos de las organizaciones sanitarias».

La gestión del cambio no es nueva en el marco de las empresas y la industria en general, y en su práctica a lo largo de los últimos años se ha acumulado experiencia y conocimientos que proporcionan una

base de referencia técnica y herramientas de gran ayuda. En el ámbito sanitario hay que tener en cuenta las características propias del sector, su complejidad y su relativo retraso en la adopción de las nuevas tecnologías.

La gestión del cambio requiere esfuerzos estructurados, conocimientos, recursos y dotes de gestión. Uno de los problemas fundamentales es la resistencia al cambio por parte de los actores involucrados. Otro aspecto importante es la falta de control sobre los factores externos y la existencia de un buen número de incertidumbres en el entorno. La acción de la gestión de cambio no debe escatimar esfuerzos en el desarrollo de la comunicación y en la formación (Monteagudo Peña, 2004).

Los nuevos enfoques de futuro hablan de cambio continuo, organizaciones del conocimiento basadas en el aprendizaje y nuevas formas de prestación de servicios sanitarios.

7.6.1 CARACTERÍSTICAS DEL CAMBIO EN EL SECTOR SANITARIO

La gran corriente del cambio actual se apoya en dos vectores principales: la reforma sanitaria y la sociedad de la información. Con un poco más de detalle, se pueden identificar las siguientes líneas de impulso del cambio:

— Reforma sanitaria: separación de las funciones de planificación, ordenación, contratación y provisión de los servicios.

— Innovación de los servicios: nuevo planteamiento de las prácticas sanitarias.

— Incorporación de avances científicos y tecnológicos clínicos: convertir el conocimiento y el dominio de técnicas en un valor. Excelencia científica y clínica.

— Implantación de tecnologías de la información y las comunicaciones: infraestructura para el trabajo en red. Desarrollar e-Salud.

— La información como recurso corporativo estratégico (Monteagudo Peña, 2004).

El dominio de la información como recurso estratégico requiere modelar las necesidades de información de la organización a partir de las responsabilidades funcionales asignadas a los actores de los procesos. Supone identificar y comprender los elementos de actividad médica, gestión y de relación con el paciente. Para ello es importante comprender y prever las posibilidades de las nuevas tecnologías informáticas y de comunicaciones, y de sus aplicaciones en telemática sanitaria, sumando su gestión a los objetivos estratégicos de la organización.

El sector sanitario tiene características muy distintas a otros sectores, y por tanto en la gestión de cambio no se puede aplicar los mismos criterios ni extrapolar directamente las experiencias de otros sectores económicos o industriales. Aun cuando se posea experiencia en el propio sector, hay que ser cautos con las recomendaciones emanadas del análisis o de los estudios realizados en otros países con estructuras sanitarias y modelos de financiación diferentes al español. También hay que tener en cuenta los elementos culturales ligados a comportamientos y relaciones de los usuarios y profesionales en cada entorno local (Monteagudo Peña, 2004).

La gestión del cambio significa estar inmerso en la realidad y resolver cuestiones prácticas en un entorno dado. Es esencial contar con el conocimiento y experiencia real del entorno, el conocimiento teórico es muy importante, pero la práctica del cambio exige algo distinto que no se puede aprender en un marco exclusivamente académico.

7.6.2 LA RESISTENCIA AL CAMBIO

Entre los problemas con que se enfrenta la gestión del cambio se debe mencionar la resistencia. Los cambios en una organización siempre implican temores en todas las personas, desde la dirección al personal auxiliar. Estos temores se deben a la incertidumbre y pérdida de control que acompañan a la nueva situación, así como a la falta de confianza, ruptura de la rutina, pérdida de derechos adquiridos y en general, al miedo a lo desconocido. Además, no se sopesan de la misma forma las expectativas de obtener beneficios a largo plazo y los sacrificios requeridos a corto plazo (Monteagudo Peña, 2004).

A medida que la presión del cambio se está generalizando en las organizaciones sanitarias, se está produciendo una resistencia cada vez mayor ante cada nueva iniciativa, especialmente en organizaciones ya arraigadas hace tiempo y con antecedentes de experiencias de cambio no siempre motivadoras. Por ello, los expertos coinciden en señalar que uno de los aspectos decisivos, con el que hay que contar en cualquier situación de gestión del cambio, es la resistencia a éste por parte de los profesionales sanitarios.

7.6.3 PROGRAMA DE FORMACIÓN

Otro elemento fundamental que debe incluir el plan de gestión de cambio es un programa apropiado de formación y educación. El cambio en la sanidad implica la introducción de nuevas infraestructuras y herramientas. La utilización masiva de las TIC está modificando la forma en que los profesionales desempeñan su actividad drásticamente. El dominio de las nuevas herramientas requiere esfuerzos adicionales de aprendizaje y la adquisición de nuevas habilidades. Gran parte del rechazo a la innovación proviene de prejuicios debidos al desconocimiento y a la falta de dominio de las nuevas tecnologías.

Ahora bien, el programa de formación no consiste simplemente en ofrecer un conjunto de cursos sobre el último programa informático, hay que adecuarlo en tiempo y contenido a la estrategia del cambio, optimizando la curva de aprendizaje de la organización. Señala Monteagudo Peña (2004:510) que «los programas de formación deben integrarse en políticas de largo alcance de gestión y potenciación de los recursos humanos, con esquemas de formación continua y en el puesto de trabajo».

7.7 **MODELO COMPUTACIÓN EN LA NUBE**

El *Cloud Computing* es un término que en los últimos años ha resonado en todas las instancias empresariales y que está causando un cambio de modelo en la forma de trabajo cotidiano de todas las instituciones incluyendo las instituciones de salud. Tiene varias traducciones al español como ser Computación en la nube, Computación en nube o Informática en la nube o Informática en nube.

Sin embargo, para conocer la definición de *Cloud Computing*, debe entenderse que la nube es el conjunto «infinito» de servidores de información (computadoras) desplegados en centro de datos, a lo largo de todo el mundo donde se almacenan millones de aplicaciones Web y enormes cantidades de datos *(big data)* (Joyanes, 2012).

Muchas veces los términos «nube» e «internet» se utilizan como sinónimos, pero la nube es algo más que Internet. La nube es el espacio donde se utiliza cualquier tipo de tecnología disponible mientras se necesita y ni un minuto más. Una de las características primordiales de la nube es que no se instala ningún programa adicional en la computadora, ni se paga por dicha tecnología cuando ésta no es utilizada, solo se paga cuando se utiliza o se ejecuta la aplicación e incluso existe la posibilidad de utilizar este servicio de forma gratuita.

Es necesario aclarar que la nube puede ser infraestructura o software. La nube cuenta con dos conjuntos de modelos:

— *Modelo de despliegue:* Se refiere a la localización y gestión de la infraestructura de la nube y puede presentarse bajo cuatro (4) posibles formas: nube privada, nube pública, nube hibrida y nube comunitaria.

— *Modelo de servicio:* Son los tipos de servicios específicos a los que se puede acceder en una plataforma *cloud computing* y puede ser: Software como servicio, Plataforma como Servicio e Infraestructura como Servicio.

— En este sentido, el servicio en la nube cumple con tres (3) criterios:

- El servicio es accesible vía navegador Web (no propietario) o servicios Web.
- No se necesita ninguna inversión para comenzar a funcionar.
- Se paga solo cuando se utiliza y mientras se utilice.

Habiendo resumido de manera general lo que es la nube, se puede adentrar en la definición de *cloud computing*.

La computación en la nube es un término que representa un nuevo modelo de informática y que es la evolución de un conjunto de tecnologías que afectan al enfoque de las organizaciones y empresas en la construcción de sus infraestructuras de TI (Joyanes, 2012).

Analizando la realidad de lo que establece el *cloud computing*, se puede inferir que no incorpora nuevas tecnologías, lo «mágico» del *cloud computing* es que integra tecnologías ya existentes, que son potentes e innovadoras, y genera un nuevo modelo y arquitectura de la Web. El Instituto Nacional de Estándares y Tecnologías de Estados Unidos de Norte América ha definido al *cloud computing* como «un modelo que permite el acceso bajo demanda y a través de la red, aun conjunto de recursos compartidos y configurables (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con esfuerzo mínimo de gestión e interacción con el proveedor del servicio. Este modelo en nube promueve la disponibilidad y está compuesto por cinco características específicas, tres modelos de servicio y cuatro modelos de implantación» (NIST, 2011).

Las cinco (5) características clave que comprende el *cloud computing* son:

— Acceso ubicuo a la red.

— Servicio medido.

— Autoservicio bajo demanda.

— Elasticidad rápida.

— Agrupación de recursos independientes de la posición (Joyanes, 2012).

Los tres (3) tipos de servicios que otorga el *cloud computing* son: las aplicaciones, los sistemas operativos y sistemas físicos. Sin embargo, estos tres (3) modelos de servicio comúnmente son conocidos como:

— Los servicios de aplicaciones (*Software as a Service*–SaaS)

— Los servicios de plataforma (*Platform as a Service*–PaaS)

— Los servicios de infraestructura (*Infraestructure as a Service*–aaS)

Las nubes pueden ser clasificadas de diversas maneras y según los criterios que sean de mayor interés; sin embargo, la normativa española de protección de datos las clasifica de acuerdo a la forma en que afectan dichas modalidades de implementación al tratamiento de datos de carácter personal, teniendo así:

— *La nube pública:* cuando el proveedor de servicio proporciona sus recursos de forma abierta a cualquier entidad.

— *La nube privada:* cuando una entidad realiza la gestión y administración de sus servicios en la nube para las partes que la forman sin que en la misma puedan participar entidades externas y manteniendo el control sobre ellas.

— *Otros modelos:* en los que se encuentran las soluciones intermedias como las nubes hibridas que ofrecen algunos servicios de forma pública y otros de forma privada; las nubes comunitarias cuando los servicios son compartidos en una comunidad cerrada; las nubes privadas virtuales que en realidad son nubes públicas en las que se implementan garantías adicionales de seguridad (AEPD, 2013).

Se pueden distinguir, a simple vista, los beneficios más inmediatos de la utilización del *cloud computing*: reducción de costos, la simplificación de las operaciones, la mayor flexibilidad de acceso a datos y la reducción del mantenimiento de las aplicaciones (Bustamante, 2013).

Sin embargo, Bustamante Donas (2013:43-49) propone un análisis sobre los dilemas éticos y políticos en el modelo de *cloud computing* en donde enmarca las siguientes vulnerabilidades que este sistema presenta:

— Se introduce un nuevo factor de brecha digital, lo que hace más necesario que nunca la universalidad de acceso a la red y la garantía de un adecuado ancho de banda.

— La fiabilidad se convierte en un elemento clave, ya que aumenta la fragilidad de subsistemas vitales para el sostenimiento del sistema social.

— Para no convertirse en una herramienta de control social, el cloud computing tendrá que desarrollar una nueva arquitectura más democrática.

— La deslocalización de la información, es decir, que se producirá una extraterritorialidad de las leyes.

— Las amenazas a la privacidad e integridad de la información.

— La desespecialización de los usuarios y el mito de la transparencia.

— Las amenazas a la neutralidad de la red.

— La necesidad de una mayor descentralización de la red.

— La vulnerabilidad de los agentes dominantes del cloud computing frente al poder de los estados centrales.

No es de negarse que las ventajas de este modelo sean claras y evidentes, pero tampoco evita que existan algunos problemas éticos que tienen que ver con factores técnicos y de gobernanza.

Los riegos específicos que deben afrontarse cuando se realiza el uso de servicio de *cloud computing* se pueden agrupar en dos grandes categorías: la falta de transparencia sobre las condiciones en las que se presta el servicio y la falta de control del responsable sobre el uso y la gestión de los datos personales por parte de los agentes implicados en el servicio (AEPD, 2013).

En el campo de la salud, uno de los riesgos más prominentes es la privacidad de los datos. Como ya se ha visto anteriormente, los datos tratados por los servicios de *cloud computing* pueden encontrarse en cualquier lugar del mundo o centro de datos, lo que supone un riesgo incluso legal sobre la aplicación extraterritorial de las normas nacionales. Al encontrarse la infraestructura de comunicación en un territorio determinado, se encuentran bajo el control de sus legislaciones nacionales a pesar de que el flujo de información es cada vez más globalizado, ocasionando que esas legislaciones nacionales se conviertan en leyes extraterritoriales y que lleguen a afectar a los usuarios del servicio independientemente de su nacionalidad.

Una posible solución a este riesgo es la implementación de políticas de privacidad que permitan evaluar el tratamiento y los niveles de protección de los datos almacenados en la nube y la posibilidad de verificar las condiciones en las que se presta el servicio.

Asimismo, la seguridad de la información en la nube se hace fundamental para su desarrollo y utilización en el campo de la salud. Este servicio debe ajustarse a los principios fundamentales que soportan el aseguramiento de los sistemas de información en la nube, como ser: la confidencialidad, integridad, disponibilidad, autenticación autorización, auditoria, responsabilidad y privacidad (Joyanes, 2012).

7.8 BIG DATA

Dado el gran crecimiento en los últimos años de las operaciones, servicios, aplicaciones y cualquier evento ocurrido mediante el Internet, se ha producido un nuevo término que al igual del *cloud computing*, ha revolucionado en el ámbito informático.

El *Big data* consiste en un nuevo modelo da datos que se extiende por todo el mundo y que almacena las enormes cantidades de datos que se están creando en los últimos años. Estos proceden de todas partes de mundo y almacenan diversas formas de información: mapas digitales, comentarios en las redes sociales, imágenes digitales, audio y video *streaming*, GPS, datos del clima y muchos otros que por el pasar del tiempo van creciendo (Joyanes, 2012).

Es increíble pensar que hace menos de veinte (20) años los discos flexibles o disquetes almacenaban *kilobytes* y ahora se acuña la idea del manejo de *Petabytes* (1000 *Terabytes*) que se almacenan en la nube.

La capacidad del ser humano para capturar, almacenar y comprender las cantidades masivas de datos, está cambiando la ciencia, la medicina, el comercio y todas las áreas donde el hombre se mueve. Conforme se aumenta la colección de hechos, imágenes e información, también crece la oportunidad de encontrar respuestas a preguntas fundamentales.

Las organizaciones de salud, tanto públicas como privadas, pueden aprovechar las ventajas de grandes bases de datos, al igual que las farmacéuticas, haciendo un análisis general de la información disponible, se pueden detectar tendencias y tomar decisiones anticipadas para evitar problemas mayores, como puede ser, identificar las tendencias que dan lugar a una epidemia (Sevy, 2015).

CAPÍTULO VIII
MARCO PRÁCTICO DE LA INVESTIGACIÓN

8.1 ANTECEDENTES DEL MARCO PRÁCTICO

Cabe señalar que una deficiencia que se presenta en Bolivia es el acceso a la información, la misma que no está disponible en los sitios *web* oficiales; algunas instituciones del ámbito público o privado no cuentan con Memorias institucionales anuales para poder acceder a la información razón por la cual se ha tenido que recurrir al envío de notas formales a las entidades del sector público y privado para conseguir una entrevista con los actores claves.

Para conocer el estado del arte del manejo y archivo de la Historia Clínica en soporte papel, proyectos emprendidos de Historia Clínica Electrónica y la implementación de las Tecnologías de Información y Comunicaciones (TIC) en el ámbito sanitario se realizan entrevistas a funcionarios claves del Sistema Nacional de Salud de Bolivia (subsector público, seguridad social y privados con y sin fines de lucro).

En el subsector público se destacan: la Dirección General de Planificación del Ministerio de Salud, Sistema Nacional de Información en Salud (SNIS) y Programa VIH-SIDA; en el subsector de seguridad social, al Seguro Social Universitario (SSU) manejo y archivo de la historia clínica en papel, Caja de Salud de la Banca Privada (CSBP) y Corporación del Seguro Social Militar (COSSMIL), estas dos últimas están implementando la historia clínica electrónica en consulta externa y hospitalización; en el subsector privado, se ha considerado al Hospital Arco Iris, establecimiento de salud sin fines de lucro, que también ha implementado la historia clínica electrónica en hospitalización desde hace 2 años.

Entre los actores TIC del actual Gobierno, se han realizado entrevistas a la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) para conocer el servicio de certificado y firma digital y actividades que desarrollan en implementación del Gobierno Electrónico; a la Empresa Nacional de Telecomunicaciones

(ENTEL) para conocer la implementación de los Telecentros y la utilización de servicios del satélite boliviano Túpac Katari y a la Dirección General de Gobierno Electrónico del Ministerio de Planificación del Desarrollo a cargo de la socialización del Plan de Gobierno Electrónico.

Entre los actores TIC del ámbito privado, se realiza una entrevista a la Asociación de Bancos Privados de Bolivia (ASOBAN) para conocer el servicio de certificación digital que presta desde 2002.

A continuación, se transcriben las entrevistas más relevantes realizadas para propósitos de la presente investigación; cabe mencionar que no se incluyen todas por el espacio que representaría en el presente documento. Sin embargo, se ha previsto cuidadosamente incluir al total de actores claves que aportaron información para crear una visión panorámica del ámbito sanitario en Bolivia, de manera general, y en la ciudad de La Paz, de manera particular.

Por lo antes expuesto, se ha considerado que el mejor instrumento para recabar información sea la entrevista no estructurada. En algunas entrevistas se organiza la información en los tres (3) ejes principales de la investigación: 1) Protección de Datos Personales en el ámbito sanitario, 2) Historia Clínica Electrónica (Expediente Clínico) y 3) Seguridad de la Información.

Tabla 13. Entrevistas a actores claves del ámbito sanitario y actores TIC

	Entidad	Tema	Nombre y cargo	Fecha
Subsector Público	Ministerio de Salud	Dirección General de Planificación	Dr. Ronal Machaca	21/07/2015 04/08/2015
	Sistema Nacional de Información en Salud (SNIS)	SNIS-VE	Rocco Abruzzese Responsable Información, Producción de Servicios Nivel I	17/06/2015 24/06/2015
		SNIS	Ing. Jorge Bailey e Ing. Gabriel Jiménez	17/06/2015
		Software de Atención primaria en Salud (SOAPS)	Ing. Mauricio Bustillos	23/07/2015
		Sistema de Información Clínica Estadística (SICE)	Ing. Gabriel Jiménez	03/08/2015
		Sistema de Información Administrativa Financiera (SIAF)	Ing. Gabriel Jiménez	27/08/2015
	Programa VIH-SIDA	Centro Departamental de Vigilancia y Referencia (CDVIR)	Dr. David Segurondo Responsable CDVIR La Paz	20/07/2015 27/07/2015

Subsector de la Seguridad Social	Seguro Social Universitario - SSU	Historia Clínica	Jaime Riveros Encargado de Bioestadística	10/09/2015
		Manejo Historia Clínica	Lic. Sonia Apaza Jefe de Enfermeras a.i.	14/10/2015
		Archivo Historia Clínica	Lic. Elizabeth Saravia Encargada de la Unidad de Admisión, Archivo y Fichaje	14/10/2015
	Caja de Salud de la Banca Privada - CSBP	Historia Clínica Electrónica	Dr. Gonzalo Maldonado Director del Hospital Regional La Paz Médico Pediatra	04/03/2015 30/07/2015
		Historia Clínica Electrónica	Dr. David Martínez Médico Traumatólogo	22/07/2015 24/07/2015
		Software Médico y Sistema Administrativo Médico - SAMI	Dra. Tania Cherro Responsable Software Médico	25/08/2015
	Corporación del Seguro Social Militar (COSSMIL)	Archivo Historia Clínica	Lic. Katia A. de Auza Jefe de Archivo Clínico	25/09/2015 30/09/2015
		Sistema Integrado de Seguimiento Hospitalario a Pacientes - SISHAP	Coronel Grover Quiroga Director Nacional de Sistemas	04/11/2015
Subsector Privado	Hospital Arco Iris	Historia Clínica Electrónica – OPEN HAI	Ing. Julio Alarcón Jefe Unidad de Sistemas	04/08/2015 07/08/2015
		Historia Clínica Electrónica – OPEN HAI	Dr. Igor Salvatierra Adjunto Enseñanza Dirección de Enseñanza e Investigación	01/09/2015
		Archivo de la Historia Clínica	Sr. Rubén Heredia Auxiliar de Archivo	08/09/2015
Actores TIC	Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB)	Firma Digital	Lic. Kantuta Muruchi Encargada de Planificación y Proyectos	14/08/2015
		Firma Digital	Ing. Sylvain Lesage Jefe de la Unidad de Innovación y Desarrollo	02/09/2015
	ENTEL	Telecentros	Ing. Rolando Álvarez Jefe de la Unidad de Telecentros	28/07/2015
			Ing. Wilson Cuellar Profesional de Desarrollo Rural	28/07/2015
	Ministerio de Planificación del Desarrollo	Dirección General de Gobierno Electrónico	Ing. Rodrigo Siles Director General de Gobierno Electrónico	29/09/2015
	Asociación de Bancos Privados de Bolivia (ASOBAN)	Administradora de Cámaras de Compensación y Liquidación – ACCL S.A.	Ing. Ricardo Primintela Administrador de Sistemas	21/09/2015
Ecuador	Médica Salubrista	Historia Clínica Electrónica Ecuador	Dra. Patricia Coral Médica Salubrista	03/07/2015

Fuente de elaboración: Propia.

8.2 SECTOR PÚBLICO

8.2.1 MINISTERIO DE SALUD - DIRECCIÓN GENERAL DE PLANIFICACIÓN

Sector: Público	Nombre: Dr. Ronal Machaca
Institución: Dirección General de Planificación	Antigüedad: 6 meses
Cargo: Jefe de la Unidad de Planificación	Fecha: 21/07/2015 y 04/08/2015

8.2.1.1 La atención médica en los establecimientos de salud del sector público

El Jefe de la Unidad de Planificación señala que la historia clínica digital facilitaría la actual forma de atención médica en el establecimiento de salud, puesto que cuando una persona se encuentra enferma y asiste a este lugar debe seguir algunos pasos para ser atendido como ser el llenado de formularios, esperar que los mismos sean aprobados y posteriormente pueda ser atendido en el área donde este así lo requiera. De acuerdo a las recomendaciones de la Organización Mundial de la Salud (OMS) y de la Organización Panamericana de la Salud (OPS), el médico debe atender a un paciente por un lapso de treinta (30) minutos, lo que en la actualidad no se cumple debido a la carga horaria del médico que es de seis (6) horas al día (por ejemplo de 08:00 a 14:00); esto significa que solo se lograría atender a un promedio de siete (7) personas por día, siendo esta cantidad muy baja dada la demanda de atención que existe día a día en los distintos establecimientos de salud, hoy se distribuyen alrededor de veinte (20) fichas. Por otra parte, el médico debe además registrar la atención médica en cuadernos de acuerdo al tipo de seguro, por ejemplo, seguro para el adulto mayor, para la mujer, para el niño; por consiguiente, de la media de quince (15) minutos para la consulta, el médico ocupa diez (10) minutos solo en el registro de datos en el cuaderno sin haber siquiera tocado al paciente.

Bolivia cuenta con cuatro (4) tipos de establecimientos de salud:

— Primer Nivel, cuenta con Centros de Salud, Centros de Salud con Internación y Centros de Salud Integral; cuentan con un médico general, auxiliar de enfermería. La dirección de los establecimientos está a cargo del Gobierno Municipal.

— Segundo Nivel, cuenta con cuatro (4) especialidades básicas: Pediatría, Cirugía, Gineco-obstetricia, Anestesiología, y Medicina General. La dirección está a cargo del Gobierno Municipal.

— Tercer Nivel, tiene todas las especialidades y la dirección está a cargo de la Gobernación.

— Cuarto Nivel, cuenta con centros de investigación. Estos serán construidos para atender enfermedades poco conocidas. La dirección está a cargo del Gobierno central.

La capacidad de atención de estos establecimientos de salud debería estar establecida de acuerdo al nivel de resolución. En muchos casos el paciente acude a un Centro de Salud de Segundo Nivel o de Tercer Nivel cuando el mal que lo aqueja solo es un dolor de cabeza o un resfrío común, este paciente podría ser atendido en un Centro de Salud de Primer Nivel. En Bolivia no existe restricción para que el paciente sea atendido en el Segundo o Tercer Nivel sin haber pasado por el Primer Nivel. En el Hospital Boliviano Holandés[95] de la ciudad de El Alto, se puede observar que hay muchos niños que van para ser atendidos por un resfrío, cuando deberían ir a un Centro de Salud de

---

[95] Página Siete (2015), desde diciembre, el hospital Boliviano Holandés –ubicado en Ciudad Satélite– de El Alto dejará de atender diferentes especialidades y se convertirá en materno-infantil. Sus médicos de otras especialidades cubrirán el déficit de profesionales que tiene el Hospital del Norte, informó el SEDES. En cuanto a categorización, actualmente el hospital Boliviano Holandés –que es considerado de segundo nivel– trabaja como si fuese de tercer nivel. Otro de los problemas es el inadecuado uso de infraestructuras. Mientras en el hospital Boliviano Holandés los médicos pelean por entrar a una de las dos salas de quirófano, en el Norte no se usa ni una de las seis salas de quirófano. «*Hospital Boliviano Holandés será exclusivamente materno – infantil*» [en línea]: http://www.paginasiete.bo/sociedad/2015/11/5/hospital-boliviano-holandes-sera-exclusivamente-materno-infantil-75885.html [Consulta: 25/09/2015].

Primer Nivel. Sin embargo, la atención en el hospital debería ser prioritaria para los niños del área rural con neumonía, desnutrición crónica o deshidratación. En cambio, se puede observar que los Centros de Salud de la correspondiente Red, en este caso la Red Holandés o Red Los Andes, están vacíos. Por lo tanto, es necesario trabajar fuerte en la promoción y educación en salud ya que el paciente no conoce sus derechos, considera que el especialista es el único que puede resolver el problema de salud que le aqueja, cuando éste podría, sin ningún inconveniente, ser atendido en un Centro de Salud de Primer Nivel, pero el paciente siente desconfianza de este nivel. Por lo antes expuesto, todos estos puntos dificultan la atención médica para el paciente.

Por todo esto, con la Historia Clínica Digital se pretende fortalecer la utilización de la referencia y retorno del paciente (antes denominado contrarreferencia), entendiendo que la referencia se presenta cuando el médico de primer nivel refiere a un paciente para que sea atendido en un establecimiento de segundo nivel para una operación porque tiene mayor resolución; el retorno se presenta cuando el paciente ha sido atendido en el establecimiento de segundo nivel y lo retorna al Centro de salud del primer nivel para su seguimiento y recuperación. Lo que se pretende es que ningún ciudadano sea atendido en un establecimiento de salud de segundo nivel si no presenta la boleta de referencia de primer nivel.

En cuanto al desarrollo de actividades de estos establecimientos de salud en los tres (3) niveles, existen limitaciones de recursos económicos, infraestructura y equipamiento, lo que produce deficiencias en la atención a la población demandante. También es importante resaltar que alrededor del 80% de las personas que acuden a los establecimientos de salud deberían ser atendidos en uno de Primer Nivel; sin embargo, las personas acuden directamente a hospitales de Segundo y Tercer Nivel.

Se puede evidenciar que se carece de un componente de promoción de la salud; esto se traduce en que la persona debe asumir su rol en el momento en el que se enferma y visitar el establecimiento de salud correspondiente, y no esperar a que la enfermedad agrave para visitar al médico y ser atendido en emergencias.

Es frecuente en el área rural que la mujer embarazada espere hasta último momento para asistir al establecimiento, cuando debe-

ría tomar las previsiones e ir horas antes, más aun cuando es primeriza, ya que el parto puede tardar de 9 a 12 horas. Sin embargo, las mujeres llegan en las últimas consecuencias teniendo que ser atendidas en el automóvil, la camilla, el pasillo e incluso en el piso del establecimiento.

Otra conducta que se presenta en el área rural es que en los pueblos o ciudades intermedias, el día establecido para las ferias de venta de productos, es aprovechado también para hacer visita al médico; por ejemplo, en la ciudad intermedia de Caranavi de la ciudad de La Paz, la feria es el día miércoles; en Chulumani es el sábado; lo que ocasiona que esos días la atención en el establecimiento colapse y se generen quejas por parte de los pacientes; lo paradójico es que el resto de la semana el establecimiento se encuentra vacío.

Otro problema que se presenta en los hospitales de Tercer Nivel es que éstos no cuentan con médicos especialistas para la atención de los pacientes; si bien hay médicos que hacen su especialidad en el exterior, algunos se quedan a trabajar en el exterior porque les ofrecen mejores oportunidades; en el caso de los médicos que vuelven al país, éstos ingresan a trabajar en hospitales que no cuentan con el equipamiento necesario para ejercer su especialidad.

Finalmente, la inversión que ejecuta el Gobierno en el área de la salud es del 11%, siendo éste el único ingreso económico en el sector público de la salud, además del presupuesto que es asignado por parte de las gobernaciones y de los municipios.

8.2.1.2 **Sistema Único de Información de Salud (SUIS)**

La implementación de la Historia Clínica Digital es un tema nuevo para el sector salud (de) Bolivia, siendo que existen diversos sistemas de información a nivel nacional, considerando que existen varios sistemas dentro de un sistema macro y dentro de ellos existen subsistemas como el subsector público, subsector de seguridad social conformados por la Cajas Nacional de Salud, Seguro Social Universitario, Seguro de las Fuerzas Armadas (COSSMIL), todos estos autónomos; y el subsector privado conformado por establecimientos de salud con y sin fines de lucro como la iglesia, las ONG, cada uno de estos subsistemas que deberían reportar algún tipo de información al

Sistema Nacional de Información en Salud (SNIS); pero en la actualidad solo reporta el subsector público, algo el subsector de seguridad social y muy poco o nada el subsector privado.

Lo difícil en Bolivia es visualizar el modo de atención médica al paciente y el suministro de medicamentos que se le da en forma gratuita al paciente, siendo que hay muchos factores que involucran estos hechos y que llevan a este tema a una problemática.

Por lo mencionado, el Sistema Nacional de Información en Salud (SNIS) del Ministerio de Salud está incursionando en una reingeniería del SNIS cuyo objetivo es englobar a todos los sistemas y subsistemas existentes a nivel nacional.

Este Sistema Único de Información de Salud (SUIS) es una propuesta de la Ministra de Salud cuya implementación está considerada hasta la gestión 2020. El objetivo del SUIS es tener una plataforma virtual única en la que se otorgue un código a una persona, el mismo que estará inmerso dentro de la Cédula de Identidad; el Servicio General de Identificación personal (SEGIP) junto con el Ministerio de Salud han considerado viabilizar esta idea, considerando que este documento es indispensable en el diario vivir del individuo desde que nace hasta que fallece; con esto se lograría que cualquier persona pueda acudir a cualquier establecimiento de salud donde se tenga registrada su Historia Clínica Digital.

El Ministerio de Salud pretende que la nueva Historia Clínica Digital del Sistema Único de Información de Salud (SUIS) sea desarrollada desde el punto de vista del médico que es quien está en contacto con el paciente y no así desde el punto de vista del informático, que hace el desarrollo, esto en consecuencia de la implementación de ciertos sistemas de información en salud que son más estadísticos y administrativos que clínicos como el SOAPS, SICE y SIAF.

La historia clínica digital debe permitir al médico, enfermera y personal administrativo del establecimiento de salud, puedan insertar los datos del paciente de forma fácil; debe ser una herramienta de trabajo, un sistema de información amigable para que su implementación sea un éxito.

Para el análisis, diseño e implementación del SUIS y la historia clínica digital se ha de considerar la experiencia de otros establecimientos de salud a nivel nacional e internacional; también se ha solicitado el apoyo financiero a diversas organizaciones e instituciones

internacionales como el Banco Interamericano del Desarrollo (BID), Agencia Española de Cooperación Internacional (AECID), FOREDES de Bélgica y Organización Panamericana de la Salud (OPS).

El Sistema SAMI de la Caja de Salud de la Banca Privada (CSBP) es un sistema bastante amigable, pero en relación a la capacidad de atención de establecimientos, el sector público tiene alrededor de 3.800 establecimientos de salud, mientras que la CSBP cuenta con alrededor de doce (12). El Sistema que se vaya a desarrollar debe tener una gran capacidad para la atención de esa cantidad de establecimientos de salud y pacientes, desde los 5 a 59 años, que no cuentan con ningún tipo de seguro.

La persona que ha sido contratada para realizar el diagnóstico y elaborar la propuesta del SUIS es una profesional médica con experiencia nacional e internacional en atención primaria, se espera que hasta diciembre de 2015 se pueda contar con el documento.

Con relación a su participación en el Comité Plurinacional de Tecnologías de Información y Comunicación (COPLITUC), es la parte técnica del SNIS el que está a cargo del Sistema Nacional de Información en Salud los que asisten a las reuniones.

Por otro lado, en cuanto al programa de Telesalud del Ministerio de Salud, es la encargada del programa quien debe hacer conocer el alcance del programa.

8.2.1.3 **El perfil epidemiológico**

En este momento el Ministerio de Salud está elaborando el Plan Estratégico Institucional (PEI) del Ministerio de Salud 2016-2020, lamentablemente a la fecha no se realizó la Encuesta Nacional de Demografía y Salud (ENSA) para conocer el perfil epidemiológico de Bolivia; misma que se debía haber realizado en la gestión 2014. Esta encuesta está a cargo del Instituto Nacional de Estadística (INE) y el Sistema Nacional de Información en Salud (SNIS).

El Perfil epidemiológico en Bolivia cambia de acuerdo a la zona. Se tienen 3 zonas bien marcadas Altiplano (La Paz, Oruro, Potosí), Valle (Cochabamba, Sucre, Potosí) y Trópico (Beni, Pando, Santa Cruz); por ejemplo, en las zonas del Altiplano, debido a la altura, los niños presentan resfríos, diarreas; en las personas mayores, hiperten-

sión, poliglobulia. En el valle, enfermedades transmitidas por vectores como el chagas; en la zona tropical baja, dengue, malaria, leishmaniosis, chikungunya. Por otra parte, La Paz tienes los 3 pisos ecológicos; por lo tanto, se presentan más enfermedades.

La tuberculosis es una enfermedad que se presenta en los bolivianos que habitan tanto en el país como en el exterior, ya que el bacilo está presente en la persona esperando que este se active, lo que puede suceder a causa de las bajas defensas por desnutrición crónica o por vivir hacinados.

Bolivia cuenta con el Programa Nacional de Control de la Tuberculosis, el tratamiento es gratuito y dura 6 meses; todo el esquema, que consiste el tratamiento desde el diagnóstico, la atención y dotación de medicamentos, es brindado por el Ministerio de Salud. El problema que se presenta en el área rural es que la persona, que tiene conocimiento de padecer de tuberculosis, oculta su enfermedad por temor a ser discriminada por la comunidad y por los efectos colaterales de la medicación (orina roja, parálisis), lo que incide en el abandono del tratamiento.

8.3 SECTOR SEGURIDAD SOCIAL

8.3.1 CAJA DE SALUD DE LA BANCA PRIVADA

8.3.1.1 Caja de Salud de la Banca Privada – Encargada Nacional de Software Médico

Sector: Seguridad Social	Nombre: Dra. Tania Cherro Vargas
Institución: Caja de Salud de la Banca Privada	Antigüedad:
Cargo: Encargada Nacional de Software Médico	Fecha: 25/08/2015

8.3.1.1.1 *Protección de datos personales en el ámbito sanitario*

El Sistema Administrativo Medico (SAMI) es regulado por el Reglamento del 2008; el mismo enmarca principios como buena fe, con-

fidencialidad, duración de las copias magnéticas de la Historia Clínica, la garantía, la inviolabilidad, la responsabilidad institucional, la seguridad y la transparencia.

Cuando un paciente es diagnosticado con VIH, cualquier médico puede visualizar su estado en el sistema porque existe un campo denominado «observaciones nuevas», donde el personal médico debe ingresar alguna condición física del paciente que sea transversal a todas las especialidades, como es el caso de la condición serológica del paciente. Esta situación es de conocimiento del personal médico a fin de que se tomen todas las medidas de bioseguridad y para no recetarle o realizar procedimientos que dañen su condición. Esta misma previsión se la toma con los pacientes que tienen insuficiencia renal crónica, problemas en la coagulación de la sangre y otros que puedan afectar al acto médico.

8.3.1.1.2 *Historia Clínica (Expediente Clínico)*

El Sistema Administrativo Medico (SAMI) cuenta actualmente con veintiún (21) módulos, no solo del Área Médica sino también del Área Administrativa. Dadas las necesidades, estos módulos se van aumentando y actualizando.

La Historia Clínica se guarda para siempre. Todos los datos que se ingresan en el SAMI están guardados desde su creación.

El manejo de la Historia Clínica no solamente se realiza a través del sistema informático, sino también mediante papel. Esto se debe a que aún no se ha implementado, en Bolivia, la firma electrónica.

Una vez que se ingresan los datos al sistema, el usuario debe imprimir y posteriormente debe firmar. Aún se maneja un expediente clínico en papel, pero se está implementando el manejo de datos a través del sistema SAMI.

Las Historias Clínicas en papel están almacenadas en la Oficina Regional de cada Departamento, las cuales son resguardadas en una Oficina de Archivo. Una vez que el paciente solicita una cita médica, cada Regional entrega su Historia Clínica al médico que lo atenderá. Esto ocurre cuando la atención es en la Regional donde está su Historia Clínica. Cuando se solicita atención en otra Regional que no es su

Regional de registro, se utiliza la del sistema en línea para analizar la situación de los pacientes.

La visualización de la Historia Clínica está abierta a todo el personal de salud de la CSBP, independientemente de su especialidad. Esto se debe a que al ingresar a la Historia Clínica Electrónica, de manera general, la primera pantalla que se visualiza es la última consulta que tuvo el paciente, pero también está la opción para visualizar la última consulta del paciente en una determinada especialidad.

No existe una Historia Clínica Resumida (HCR), pero sí existe un Informe Médico que indica, a grandes rasgos, todo el acto médico realizado al paciente.

El sistema SAMI de Historia Clínica cuenta con dos (2) formas de mostrar el Expediente Clínico: la primera es mucho más larga, porque cuenta con los datos de la anamnesis y antecedentes; la segunda es la Hoja de Evolución que es mucho más corta. Todos estos datos son llenados por el personal médico.

La aceptación del sistema por parte del personal médico es bastante amplia; se cuenta con capacitación constante para ellos respecto a la utilización y manejo del sistema cada vez que existe una actualización o creación de un nuevo módulo.

Cuando existe la incorporación de un nuevo personal de salud, se le otorga tres (3) días de inducción en el manejo del sistema SAMI; se les otorga los manuales, las guías y se tiene un procedimiento de práctica. Esta capacitación la realizan los Encargados de Software Médico o en su defecto el personal informático. Una vez capacitados se los certifica en el manejo del sistema SAMI en sus módulos correspondientes.

La consulta dura aproximadamente quince (15) minutos, los cuales son suficientes para el llenado de los campos en la Historia Clínica Electrónica y la revisión médica al paciente. Este tiempo de consulta está determinado por el INASES.

Para fines estadísticos, el mismo SAMI coadyuva a la clasificación de las enfermedades a través de dos (2) parámetros: el primero otorgado por el Clasificador Internacional de Enfermedades CIE-10, y el segundo, por los parámetros manejados por el Ministerio de Salud de Bolivia (8 cuadernos de clasificación). Para realizar la clasificación de

las enfermedades, el sistema utiliza la estructura de datos denominada «árboles».

El paciente no puede acceder a su Historia Clínica Electrónica en línea, pero puede solicitar una copia impresa a través de una nota dirigida a la Jefatura Médica o al Administrador Regional. Generalmente no piden copia de toda su Historia Clínica, lo que más solicitan son los informes médicos. El único módulo al cual puede acceder el paciente es la solicitud de citas médicas vía *web* a través del portal de la CSBP.

8.3.1.1.3 *Seguridad de la Información*

Para el desarrollo de un nuevo módulo en el sistema, se conforma un equipo multidisciplinario de profesionales que analiza los requerimientos. En el análisis de creación de un nuevo módulo participan médicos, enfermeras, trabajo social, área de sistemas informáticos, desarrolladores de software médico y las distintas especialidades médicas. Esto debido a que existe interconsulta del paciente, es decir, que el paciente no sólo consulta a un solo médico, sino que generalmente son varias especialidades que hacen el tratamiento para cada uno de los pacientes.

Cuando existe un mal manejo de la información, de acuerdo al Reglamento Interno del Personal, se establecen sanciones que van acorde al daño ocasionado por el mal manejo de la información. Cualquier problema que surja con el manejo de accesos o de usuarios es remitido al Departamento de Recursos Humanos para que se tomen las medidas correspondientes, pero no se cuenta con un Reglamento específico de sanciones por el mal uso del SAMI.

En el Módulo de Farmacia existen controles para la entrega de medicamentos. La prescripción médica no puede ser mayor a sesenta (60) días, pues el control del paciente se realiza cada sesenta (60) días. También, en el caso de interconsulta, si un médico quiere recetar un medicamento que ya se le había otorgado al paciente, el sistema alerta de esta situación para evitar la doble prescripción.

Todos los campos que han sido llenados por el personal médico con anterioridad, a pesar de poderlos visualizar, no se pueden modificar.

El personal de enfermería no puede ingresar a la Historia Clínica Electrónica, ellos tienen un propio módulo que está desarrollado para su especialidad.

Cuando el médico desea modificar alguna información de la Historia Clínica, éste tiene un plazo de veinticuatro (24) horas para hacerlo, esto se debe a que a veces el paciente no otorga toda la información en el momento de la consulta. Pero el médico solo puede ingresar datos en un campo llamado «anotaciones», previa autorización de los Supervisores; la parte de la Historia Clínica no puede ser modificada, esto a fin de preservar la seguridad de la información ingresada en la Historia Clínica.

También existe una base de datos para auditorias que almacena todos los cambios realizados en la Historia Clínica, es así que los supervisores (Encargados de Software Médico) son los que evalúan esta situación y analizan todos los cambios y modificaciones en las Historias Clínicas.

Cada usuario tiene sus propios módulos. Se trabaja con la asignación de privilegios para cada personal de la CSBP. Ningún usuario puede acceder a otros módulos que no le fueron asignados ya que la otorgación de privilegios es personal.

Respecto a imagenología, la CSBP aún no cuenta con el sistema RIS-PAC, pero se está proyectando que para el año 2016 se adquiera este tipo de sistema.

8.3.1.2 Caja de Salud de la Banca Privada – Director de la Clínica Regional de La Paz

Sector: Seguridad Social	Nombre: Dr. Gonzalo Maldonado
Institución: Caja de Salud de la Banca Privada	Antigüedad:
Cargo: Director de la Clínica Regional de La Paz	Fecha: 04/03/2015 y 30/07/2015

Desde el año 2008, se ha mejorado el sistema informático, se tiene toda la atención médica, desde afiliación a laboratorios. Se está trabajando en informatizar la parte de hospitalización, no solamente los formularios sino todos los procesos médicos, además de instalar captación de imágenes para la historia clínica. Se cuenta con el presupuesto para lograrlo.

Las bases de datos de la Caja de Salud de la Banca Privada eran locales, pero se requiere que todo se concentre a nivel nacional para que sean de consulta, dependiendo del enfoque; si éste es operativo o normativo.

8.3.1.2.1 *Estructura y niveles*

En cuanto a estructura, la Caja de Salud de la Banca Privada tiene ocho (8) oficinas regionales, en la Oficina Nacional hay una Unidad de Software Médico que se encuentra a cargo de la Dra. Tania Cherro, Responsable Médico del desarrollo informático médico. En vista de que la historia médica será informatizada, cumpliendo con la normativa nacional, la Unidad de Software Médico traduce toda la necesidad médica a la parte informática.

Se cuenta además con una Unidad de Telemática Médica a nivel nacional con sus contrapartes regionales, en cada regional hay una unidad; entre sus funciones están el desarrollo, la estructura, las redes, el cumplimiento de estándares del campo de hardware. El software del hospital se ha desarrollado y configurado según el aumento de servicios que necesitan ser informatizados; al mismo tiempo, los datos han sido pasados en VPN (*virtual private network*) para que se tenga un buen control de la información.

Hay dos niveles nacional y regional. El nivel nacional está relacionado a lo normativo, el desarrollo, las políticas y las directrices; mientras que a nivel regional, como en los diversos establecimientos de la ciudad de La Paz, integran toda la información, trabajan con niveles de acceso, protocolos, seguridad, usuarios, perfiles y auditoría; se cuenta con un buen desarrollo de infraestructura tecnológica a nivel nacional y regional. Sin embargo, la adecuación a la normativa es un punto que está aún en desarrollo.

8.3.1.2.2 *Funcionamiento del software*

El software se encuentra en funcionamiento a nivel perfiles, se trabaja para un nivel de recolección de datos. La informatización en el hospital tiene muchas ventajas, el personal médico de la Caja de Salud de la Banca Privada ya tiene cultura informática, volviéndose incluso dependientes del sistema. El sistema SAMI se encuentra respal-

dado, lo único que se espera es el reglamento para la Firma digital. La Dra. Susan Aliaga ha presentado un proyecto llamado «papel cero» para la parte clínica, pero no se lo realiza por razones jurídicas.

El INASES aprueba, en la gestión 2005, el Reglamento para la elaboración, manejo y archivo del expediente médico o clínico en las entidades de seguridad social a corto plazo, el Reglamento se convierte en un documento oficial. Posteriormente, en 2008 se aprueba la Norma Técnica para el manejo del Expediente Clínico con el propósito de normar el manejo de un expediente clínico en papel.

El personal del área operativa no tiene dominio de esta normativa. Existe una estandarización que se cumple más en el sector público que en la seguridad social; pero el personal de estadística y de enfermería maneja estos archivos. En la Caja de Salud de la Banca Privada, por ejemplo, hay un médico para que lleve a cabo la auditoría médica.

8.3.1.2.3 *Protección de datos personales en el ámbito sanitario*

La falta de confidencialidad es una falta grave; en la CSBP, el personal que incumpla con dicha confidencialidad es sancionado con suspensión temporal de quince (15) días sin goce de haberes, treinta (30) días de suspensión sin goce de haberes y la destitución, dependiendo de cómo califica el Comité la falta. Los casos que se atendieron con mayor frecuencia fueron del área de enfermería o de instrumentación.

La CSBP fija canales para las denuncias de los pacientes, las mismas se realizan ante las autoridades regionales y se elevan a la Unidad regional de Auditoría Médica.

La historia clínica de la CSBP es privada y confidencial, pero se habilita el acceso a los médicos y enfermeras y personal de salud (interconsultas), pero la información de diagnóstico es solo médica. El paciente no puede acceder a la historia clínica electrónica.

En la CSBP ha habido casos por falta de confidencialidad; en consecuencia, se han llevado a cabo procesos internos, los que, al probarse la falta, han derivado en sumarios administrativos al personal involucrado. En el Hospital del Niño del sector público, por ejemplo, hay un Comité de Auditoría Médica, que, en base a los resultados de

sus investigaciones, otorga sanciones. Pero si esto pasa al ámbito penal, se manda al Servicio Departamental de Salud (SEDES) para que éste realice una auditoría externa.

Para que un paciente de la CSBP pueda obtener una copia de su historia clínica, el titular del seguro debe solicitarlo a través de una carta; mientras que el acceso por terceras personas se realiza por requerimiento fiscal u orden judicial (parientes, ex cónyuges, etc.) El requerimiento fiscal u orden judicial llega al Gerente General, el cual deriva a la Unidad de Auditoría Médica; esta instancia puede derivar a la Unidad de Archivo y Estadística. Si el caso fuera por una denuncia, la solicitud se realiza directamente a Asesoría Legal.

En los hospitales de segundo y tercer nivel hay un Responsable de la Unidad de Archivo y Estadística, el cual es responsable de la seguridad de los expedientes clínicos, los cuales deberían tener formación en archivística o bibliotecología, en muchos casos se contrata simplemente a un profesional de otra área.

8.3.1.2.4 *Historia Clínica (Expediente Clínico)*

Las historias clínicas deben estar en archivos centralizados, en primera instancia tiene acceso el personal de estadística; en segunda, el personal autorizado como ser de enfermería. En el Hospital del Niño existe una Unidad de Archivo y Estadística donde el médico tiene que llenar un formulario para retirar un expediente clínico. En la CSBP, el archivo y custodia de las historias clínicas activas son por cinco (5) años y las pasivas diez (10) años; pasados los diez (10) años, se pueden disponer las historias clínicas, lo que se encuentra reglamentado en el Código de Salud.

En Bolivia no se maneja aún la Historia Clínica Única. No hay, en primera instancia, por el nivel político; en segunda instancia porque hay que tener un consenso, pero no solo a nivel nacional sino también a nivel regional con sindicatos médicos. Esta Historia Clínica Única debería estar categorizada por especialidades. El Ministerio de Salud no tiene suficiente rectoría, capacidad técnica, propositiva, buen nivel de asesoramiento; no existe un estudio médico serio, ni financiamiento; el Ministerio de Salud es un Ministerio débil.

El Ministerio tiene una línea más política que técnica. Uno de los problemas es que el Sistema de Salud se ha fragmentado en público,

privado y seguridad social; en cuanto a funcionamiento, no hay un control, un estándar, por lo que el Ministerio debería delegar sus funciones a los Municipios y a las Gobernaciones.

El paciente es un sujeto pasivo, pero que sí puede obtener una copia de su historia clínica así como realizar sus citas por internet.

Existen diferentes tipos de médicos: unos con visión clínica; otros, con visión salubrista. En el primer caso, no interesa la consulta sino el paciente, la atención que se le brinda; en el segundo caso, no tienen la visión clínica, ellos necesitan su unidad equipada. En cuanto a gestión clínica en el caso de la Caja de Salud de la Banca Privada el Director de una Clínica es el que controla y hace gestión clínica, controla primero los médicos y luego las enfermeras. Lo que se quiere lograr es que los médicos hagan gestión clínica; es decir, que se cumpla el horario de seis (6) horas de trabajo, los médicos deben generar productividad. El sistema es una herramienta para poder controlar esta área de manera eficaz.

Ningún sector de salud tiene un sistema de costos, las clínicas privadas son comerciales. En el sector público, el tratamiento de un paciente lo paga el Estado siempre y cuando esté subvencionado.

La desventaja de la historia clínica electrónica es que ésta no tenga adecuadas medidas de seguridad, pudiendo quedar vulnerables los datos. Otro problema es que se caiga el sistema; el alto costo de inversión en hardware y software hace que no sea accesible. El sector público no tiene acceso a las TIC, lo cual genera instituciones de primer, segundo y tercer nivel en cuanto a la implementación de las TIC.

Los responsables del área de Sistemas de Información son dos (2) principalmente: Responsable del SAMI nacional y regionales (La Paz, Cochabamba, Santa Cruz); en cada una de estas regionales hay una Unidad de Software Médico y una Unidad de Informática que se encargan de ver la calidad del sistema, nuevos módulos. El Responsable de la Unidad Telemática está encargado de la tecnología del software.

El acceso a Internet dentro de la CSBP es restringido por máquina y usuario; vale decir, el personal tiene acceso pero con previa autorización. Sin embargo, no se otorga acceso a sitios como correos electrónicos (gmail), Facebook, etc.

Está proyectado que los pacientes también tengan acceso al Wi-Fi. Se realizan capacitaciones a través de una plataforma virtual de e-learning, se cuenta con cursos de dactilografía. Existen diferentes niveles para que el médico se capacite dos (2) veces al año.

El manejo de las TIC dentro del personal médico es aún bajo. La CSBP cuenta con infraestructura para teleconferencias, pero no se realizan por falta de cultura en el personal.

En el ámbito de seguridad, en este último año se contrató a un oficial de seguridad de la información. Dentro del personal de la CSBP, tanto los médicos como las enfermeras cuentan con un nombre de usuario y un *password*, cada uno tienen su propio perfil, con algunas restricciones para psicología, psiquiatría. El médico, por su parte, debe solicitar autorización para acceder a la historia clínica que tiene restricciones.

El esquema que se maneja es el de base de datos locales; es decir, que un médico de la ciudad de Tarija no puede ingresar a la historia clínica de un paciente en la ciudad de La Paz. Cada regional tiene sus propios servidores que reportan, de manera diaria, mediante envíos de *backups* a la Oficina Nacional para que se centralice la información en el Data Center; este es un tema de servidor y de estructura, la vigencia de derechos es nacional. La Unidad de Telemática está a cargo del hardware y software de la CSBP.

8.3.1.2.5 *Seguridad de la información*

No existe el reglamento de la Ley para implementar la firma electrónica. En el caso de la CSBP todos los datos del paciente se encuentran tanto en el sistema SAMI como en papel; la historia clínica todavía es archivada en papel con firma y sello del médico y enfermera. Bolivia no cuenta con una Entidad Certificadora autorizada para ofrecer el servicio de firma electrónica.

Una de las limitantes para la CSBP es la parte de la implementación tecnológica, internet, tabletas, son inversiones con un costo elevado. A pesar de que la CSBP tiene los recursos la inversión es bastante elevada; por otra parte, los médicos se están acostumbrando al nuevo proceso tecnológico, la historia clínica electrónica ayuda a una mejor gestión de recursos.

La CSBP no realiza auditorías informáticas de manera rutinaria, en todo caso se la realiza por problemas de seguridad o ante la compra de servidores por requerimiento.

Cuando se cae el SAMI, todo se realiza de forma manual, cada médico pasa su información a la Unidad de Informática, que es la que se encarga de cargar en el sistema la información proporcionada. El mayor tiempo de caída del SAMI en la CSBP fue de seis (6) horas (toda una mañana).

La CSBP cuenta con un Plan de Seguridad para las personas, equipos, ambientes; por reglamento, se cuenta con videovigilancia de manera permanente en pasillos, entradas, salidas a excepción de los consultorios y de los quirófanos para resguardar la confidencialidad del paciente.

8.3.1.3 Caja de Salud de la Banca Privada – Médico Traumatólogo

Sector: Seguridad Social	Nombre: Dr. David Martínez
Institución: Caja de Salud de la Banca Privada	Antigüedad: 12 años
Cargo: Médico Traumatólogo	Fecha: 22/07/2015 y 24/09/2015

La Caja de Salud de la Banca Privada (CSBP) tiene como objeto social el de contribuir a mejorar la salud y bienestar de toda su población asegurada, brindando prestaciones y/o atenciones médicas integrales, accesibles, oportunas, eficientes y eficaces, enmarcadas en principios de profesionalismo, calidad del servicio, calidez, sostenibilidad y transparencia. Para tal efecto, la CSBP otorga servicios propios y/o contratados de terceros.

La Caja de la Banca Privada tiene un registro electrónico, pero no llega a ser una historia clínica completa, porque los datos que se cargan en la computadora deben ser impresos en papel, el médico de firmar y sellar. Si bien el registro está en una base de datos, la misma está completamente restringida, ni siquiera el médico puede obtenerla; para tener la información de la historia clínica se tiene que emitir un informe solicitando el acceso, si no existiera este método de control, se tendría acceso a la información.

8.3.1.3.1 *Protección de datos personales en el ámbito sanitario*

La Caja de Salud de la Banca Privada cuenta con una Norma Técnica para el manejo del Expediente Clínico, la cual se aplica apoyada en el Reglamento del Comité de Auditoría Médica Interna en el marco de la Gestión de Calidad.

Asimismo, como parte de un sistema de control, supervisión y mejora continua, se ha dado continuidad a las siguientes actividades que ya forman parte de la gestión de la CSBP, en este sentido el hecho de confiabilidad en Bolivia se tiene que definir.

El acceso a la información de la historia clínica electrónica se otorga según la especialidad. El médico tiene derecho a ver sólo los registros de su especialidad; por ejemplo, artritis reumatoidea que afecta al corazón y al pulmón además de ser invalidante pues afecta a las articulaciones; de esta afección sí se tiene acceso, saliendo en el registro de manera inmediata como enfermedad crónica. Sin embargo, al ser una enfermedad invalidante, al menos para un funcionario bancario, la restricción de esta información debe tratarse de manera especial.

8.3.1.3.2 *Historia Clínica (Expediente Clínico)*

Hoy en día, la historia clínica electrónica SAMI tiene la ventaja de permitir al médico tener conocimiento sobre las enfermedades que padece un paciente, tales como cáncer, VHI, hipertensión arterial, diabetes, artritis reumatoide.

Los hospitales están obligados a mandar un registro de la cantidad de pacientes atendidos con patologías prevalentes como resfríos, hipertensión arterial, etc. al Sistema Nacional de Información en Salud (SNIS) del Ministerio de Salud. Sin embargo, los reportes de cantidades de enfermedades infectocontagiosas se manejan de otra manera. Es por esta razón que la historia clínica electrónica sería de gran beneficio para conocer esas patologías.

El acceso a SAMI es limitado, el paciente no puede ingresar a su propia historia clínica; sin embargo, con un usuario y contraseña puede hacer citas por internet.

El médico puede ingresar a otro perfil para obtener información pertinente al caso que atiende, justificando el porqué del acceso a la historia del paciente cuando la atención no está relacionada con su especialidad.

El registro electrónico de la CSBP es un control administrativo para el médico, el sistema no permite la impresión de la receta cuando a un paciente se le ha prescrito más de cuatro (4) medicamentos, en este caso se debe realizar un nuevo registro en el sistema. Hay datos que no pueden ser registrados en la historia clínica, pero se cuenta con otros espacios en los que sí se puede registrar información siempre y cuando esta sea pertinente y necesaria de hacer conocer.

Mediante evaluaciones al expediente clínico, seguimiento individualizado y auditorías médicas, se realizan mejoras al sistema, lo cual contribuye a un mejoramiento en la calidad de atención a los asegurados. La auditoría médica que realiza cada tres (3) meses la CSBP a la historia clínica electrónica permite mejorar la calidad de la información contenida en la misma, verifican que todos los espacios sean llenados, si se utilizan correctamente los términos, que no se dejen espacios en blanco, puntuación, otros.

La CSBP tiene dos (2) historias clínicas diferentes, una para consulta externa y otra para hospitalización (internación); estas no comparten información.

El sistema SAMI no permite el acceso de radiografías, tomografías, ecografías y otras imágenes a su base de datos, pues no se cuenta con un sistema de digitalización de las mismas, traduciéndose esto en un aspecto negativo del sistema SAMI.

8.3.1.3.3 *Seguridad de la Información*

Si un paciente con VIH-SIDA no desea que su entorno tenga conocimiento de su enfermedad, la información es registrada en la historia clínica electrónica del SAMI pero el acceso será restringido, el médico accederá a la información a través de un código esta información no puede ser divulgada.

Existen perfiles por especialidades; la parte institucional ingresa al perfil con un nombre de usuario y una contraseña. La contraseña (*password*) se utiliza como medida de seguridad, a la que no solo tie-

ne acceso el médico, también accede el médico de turno que es quien colabora con la atención del paciente en caso de hospitalización (por ejemplo en una cirugía).

La información del paciente se puede guardar en la HCE del SAMI pero no se puede imprimir. Por otro lado, existe la posibilidad del error en el llenado de la historia clínica electrónica, existen casos en los que por error humano se ingresan datos de un paciente en la historia de otro paciente, por eso es importante la impresión para poder corroborar la información introducida.

La enfermera cuenta con su propio perfil al que accede a través de un nombre de usuario y contraseña; la contraseña es un código proporcionado por la Unidad de Telemática; las enfermeras no pueden cambiar la contraseña y si por alguna razón se olvida la misma, Telemática le proporciona una nueva.

En la práctica, las enfermeras son las que mejor manejan el sistema SAMI; en muchas ocasiones son apoyo para los nuevos médicos en el llenado de los formularios y campos. Las enfermeras consideran que el SAMI tiene más ventajas que desventajas, el problema es cuando el sistema se cae por falta de energía eléctrica; en ese caso se debe realizar el llenado de los formularios en forma manual, otras veces el sistema esta lento por el tráfico de personas que utiliza el sistema. Las enfermeras que trabajan en otros establecimientos de salud valoran el sistema SAMI porque facilita su trabajo y se evita el llenado manual de la historia clínica y de los cuadernos de datos del paciente y su evolución.

8.3.2 CORPORACIÓN DEL SEGURO SOCIAL MILITAR (COSSMIL)

8.3.2.1 **Corporación del Seguro Social Militar - Jefatura de la Unidad de Archivo Clínico**

Sector: Público	**Nombre: Lic. Katia A. de Auza**
Institución: Corporación del Seguro Social Militar	Antigüedad: 12 años
Cargo: Jefe del Archivo Clínico	Fecha: 25/09/2015 y 30/09/2015

El Hospital Militar Central - COSSMIL es una entidad semi-descentralizada ya que dentro de ella existe una parte que pertenece al área militar constituyéndose el mismo en un Hospital Militar; por lo mismo, ésta es regulada por la Ley Orgánica de las Fuerzas Armadas (LOFA).

Para la implementación del expediente clínico dentro del Hospital Militar Central, se ha contemplado la aplicación de parámetros como la misión y la visión de la Unidad de Archivo «con enfoque líder en la protección de los datos del paciente, bajo la confidencialidad, resguardo y privacidad para cuyo fin debe tener una tecnología de punta que permita implementar la digitalización del sistema concretizando su uso como instrumento de trabajo e investigación».

El Hospital Militar Central - COSSMIL ha creado protocolos de archivos, es así que el sistema que maneja el hospital es diferente al de los demás hospitales del resto de las regionales de COSSMIL; la diferencia está en el archivo de la historia clínica de consulta externa y hospitalización, ambas forman parte del expediente clínico.

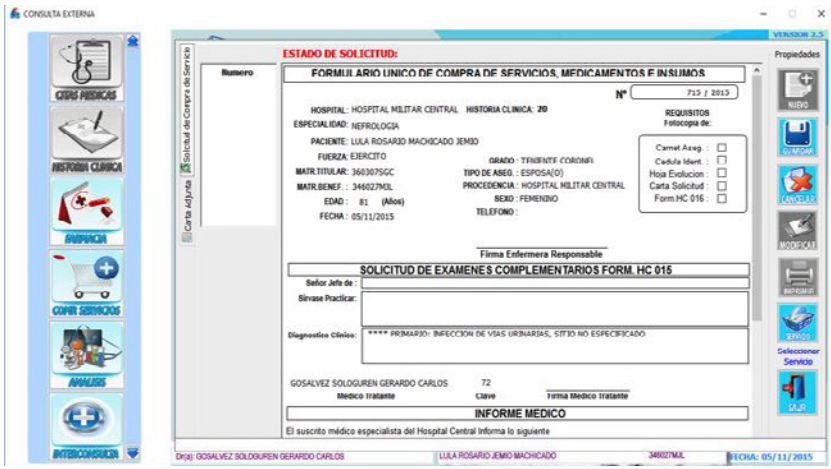

Figura 22. Vista del módulo Compra de Servicios de SISHAP

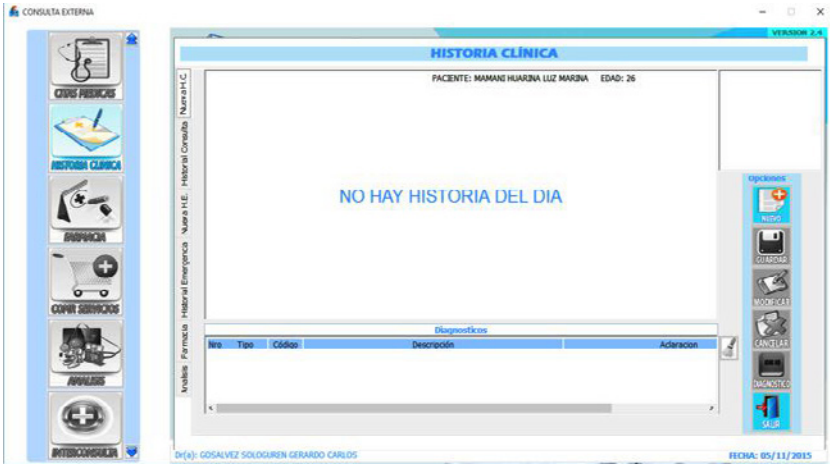

Figura 23. Vista del módulo Historia Clínica Electrónica de SISHAP

Fuente de elaboración: Corporación del Seguro Militar.

El Expediente Clínico es el conjunto de todos los documentos correspondientes a la salud del asegurado. En el Hospital Militar Central - COSSMIL se cuenta con la Carpeta Familiar que tiene un código relacionado al nombre, apellido, fecha de nacimiento del paciente titular del seguro; a la esposa e hijos se los incluye en la carpeta familiar.

La Historia Clínica es un archivo clínico que sale con boleta de control, el tipo de foliación para este documento se realiza de forma específica para consulta externa, hospitalización, laboratorios. La Unidad de Archivo ha tomado como ejemplo la foliación que realizan las enfermeras que utilizan bolígrafos de colores, por ejemplo color rojo para consulta externa, color verde para las recetas.

La Resolución Ministerial 090/2008 Norma Técnica para el manejo del Expediente Clínico es el marco legal para todos los establecimientos de salud.

Una política de la Unidad de Archivo es que ningún expediente clínico es retirado sin el registro correspondiente; el expediente clínico es un documento legal y debe tener el resguardo conforme la normativa vigente.

La Jefe de Archivo Clínico señala «cuando hay demasiado personal que tiene el acceso a la información del expediente clínico se pue-

de generar una fuga de información produciendo vulneración de la privacidad».

Dentro del sistema de manejo del expediente clínico del Hospital Militar Central se tiene un sistema de archivo diferenciado, lo que implica un conjunto de elementos que hacen un archivo completo pese al gran número de pacientes que son atendidos al día (alrededor de 1.000 pacientes) y el gran movimiento que realiza cada uno de los expedientes que se encuentran ordenados por colores, de acuerdo a las enfermedades y al diagnóstico de los pacientes.

Para realizar la apertura de una historia clínica en la Unidad de Archivo, se debe cumplir con ciertos requisitos como ser la firma de la Encargada de Archivo y el visto bueno de la Jefe de Archivo.

En la Unidad de Archivo trabajan ocho (8) personas que están divididos en dos (2) horarios; mensualmente se asignan a las personas encargadas del expediente clínico, las enfermeras que son las personas que recogen las historias clínicas; de acuerdo a ese cronograma saben a qué funcionario dirigirse para recoger y dejar las historias clínicas.

Las enfermeras deberían recoger las historias antes que empiece la atención en Consulta Externa a las 08:00 a.m., pero recién pasan por la Unidad de Archivo a las 09:00 o más tarde; la Unidad hace que las enfermeras registren con puño y letra la lista de historias clínicas que recogen y el horario para evitar reclamos de los médicos.

La Unidad de Archivo Clínico, para facilitar la atención al personal del Hospital Militar Central (enfermera, auxiliar de enfermería, médico), cuenta con dos (2), timbres uno para el personal de COSSMIL y otro para los pacientes que también pasan por la Unidad para reclamar y conocer donde se encuentra su historia clínica.

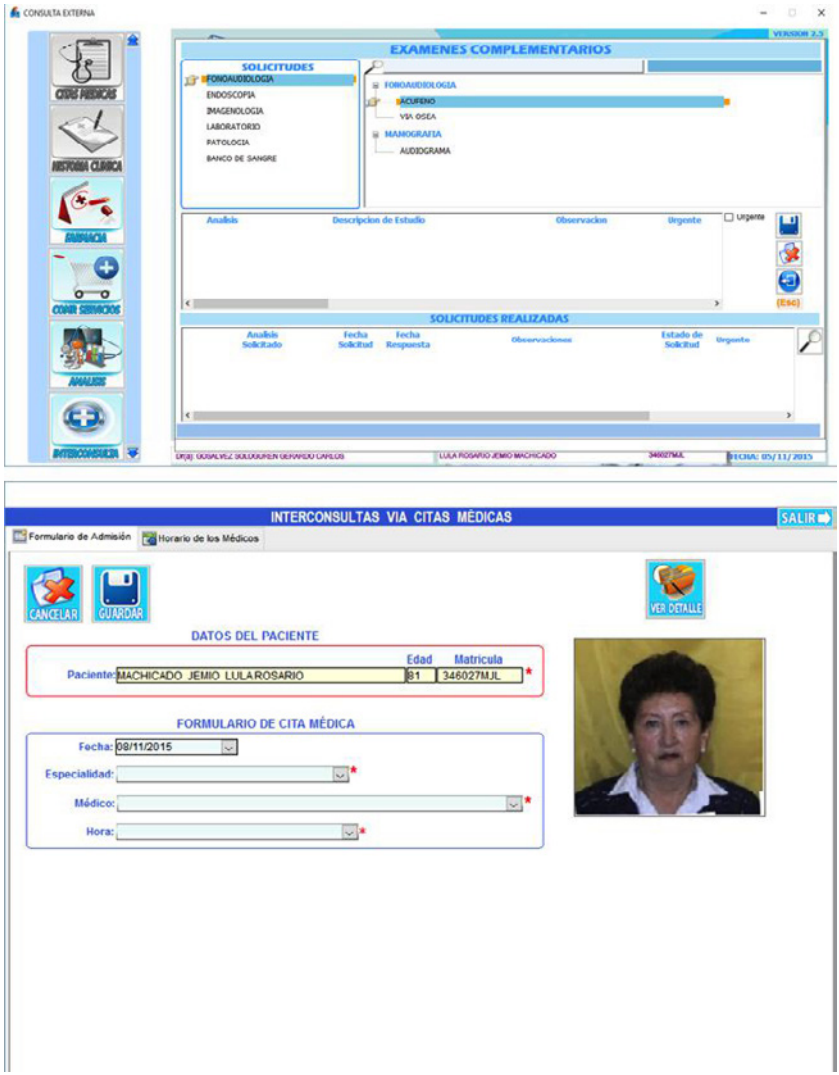

Figura 24. Vista del módulo Historia Clínica Electrónica de SISHAP

Fuente de elaboración: Corporación del Seguro Militar

La preocupación de la Unidad de Archivo es la forma en que se ha venido desarrollando el Sistema de Información Integrado de Control y Seguimiento Hospitalario (SISHAP), que puede tener medidas de seguridad para el resguardo de la historia clínica electrónica; pero la perso-

na que tenga el manejo de la misma puede manipular la información y hacer que en muchos casos lo privado y confidencial sea público.

Lamentablemente, para el desarrollo del SISHAP no ha habido coordinación con otros actores clave como la Unidad de Archivo Clínico, Auditoría Médica y otras unidades. El médico que está utilizando la historia clínica electrónica del Módulo Consulta Externa, ya no quiere volver a llenar la historia y coloca en la historia clínica en papel «ver sistema», lo cual no es correcto, más aun si está historia clínica será remitida a otro médico para la hospitalización del paciente, todavía no está implementado, en el SISHAP, el Módulo Hospitalización.

Cuando ha empezado a funcionar el SISHAP, una orden del alto mando militar a cargo del Hospital Militar Central - COSSMIL consideró pertinente destruir las historias clínicas en papel o hacer cambio con las empresas que reciclan papel por papel higiénico, a lo cual la Jefe de Archivo tuvo que oponerse y fundamentar que la historia clínica es un documento legal que respalda la atención del médico hacia el paciente existiendo una normativa nacional que señala los mecanismos para la destrucción de las historias clínicas pasivas, destrucción que se debe realizar ante la presencia de un Notario.

Cabe señalar que el Hospital Militar Central - COSSMIL ha logrado implementar el archivo del expediente clínico de forma ordenada, segura y confiable. El Instituto Nacional de Seguros de Salud (INASES) como órgano rector del seguro social a corto plazo ha reconocido el trabajo de la Unidad de Archivo Clínico y la ha invitado a dar a conocer su experiencia en el archivo del expediente clínico a otros establecimientos de salud.

8.3.2.2 Corporación del Seguro Social Militar - Dirección del Departamento de Sistemas

Sector: Seguridad Social	**Nombre: Cnel. DAEN Grover Quiroga Gutiérrez**
Institución: Corporación del Seguro Social Militar – COSSMIL	Antigüedad: 1 año
Cargo: Director del Departamento de Sistemas	Fecha: 04/09/2015

En el Hospital Militar - COSSMIL se ha desarrollado, desde la gestión 2014, el Sistema de Información Integrado de Control y Seguimiento Hospitalario (SISHAP) que tiene como objetivo satisfacer las necesidades del usuario y facilitar la atención que realiza el médico al paciente.

Falta implementar los módulos de ventas de servicios, medicina en rehabilitación y hospitalización, todo ello con el objetivo de tener mejor manejo del sistema SISHAP a nivel nacional.

El Sistema SISHAP cuenta con los siguientes módulos:

Tabla 14. Módulos de SISHAP

Módulos	
Vigencia de derechos	Emergencias
Laboratorio	Citas médicas
Consulta Externa	Nutrición
Odontología	Farmacia e Inventarios
Cardiología	Almacenes e Inventarios
Vacunas	Asignación de horarios a personal médico

El SISHAP proporciona al médico del hospital la posibilidad de incorporar, por medios electrónicos, la historia clínica de su paciente; es decir, el diagnóstico de un determinado paciente que acude al hospital para ser atendido. Al momento de ingresar al SISHAP, el médico encontrará en su perfil toda la información correspondiente a la Historia Clínica del paciente.

Para el manejo de estos módulos se realiza una capacitación previa a los médicos para que puedan manejar el sistema, la capacitación se realiza de manera general y luego personalizada a cada uno de los médicos según los problemas y las exigencias que se requieran.

En cuanto a la capacitación, el problema de COSSMIL es el escaso personal con el que cuenta en las regionales de otros departamentos; cuenta con un Suboficial que no es informático. En la oficina nacional no hay problemas porque están los funcionarios del Departamento de Informática. Por otra parte, el médico no tiene la suficiente disponibilidad de tiempo para ser capacitado en los módulos; el personal

del Departamento de Informática depende de la voluntad y tiempo del médico. En el momento que se capacita al médico para el manejo del módulo, se aprovecha para conocer las observaciones y sugerencias. Por ejemplo, a sugerencia del médico se ha incluido la edad del paciente y otros datos de interés en la historia clínica electrónica.

Es fundamental que toda la información contenida en la historia clínica que se encuentra en papel esté reflejada de igual forma la Historia Clínica Electrónica contenida en el SISHAP; con ello se busca satisfacer las necesidades exigidas por los médicos del hospital. Asimismo, el único que maneja el módulo de Consulta Externa del SISHAP es el médico del hospital quien está encargado de la atención al paciente. El acceso al sistema se realiza a través de un usuario y una contraseña. La primera vez que ingresa el médico al SISHAP se le entrega una contraseña común *(cossmil2015*),* pero para poder acceder el sistema le obliga a cambiar la contraseña, la misma que es confidencial y de conocimiento del médico. El nombre de usuario del médico está conformado por la inicial de su nombre, la inicial del apellido paterno y la inicial de su apellido materno, por ejemplo: Gerardo Gosálvez Sologuren «*ggosalvess*»; la contraseña que establezca el médico es privada y confidencial.

La información de las historias clínicas electrónicas y otros módulos del SISHAP se encuentran en servidores en el Hospital Militar Central en la ciudad de La Paz, por seguridad se realizan copias de seguridad *(back up)* de forma semanal, tienen servidores redundantes (espejos) ubicados en el mismo Departamento de Informática. COSSMIL paga la licencia del software y los antivirus.

El SISHAP se ha implementado en la ciudad de Sucre y en Puerto Suarez.

— *Módulo Venta de Servicios:* El perfil es para la persona que realiza el cobro; primero ubica al paciente, la persona tiene la posibilidad de ver el expediente clínico en papel, la justificación del acceso al expediente clínico (historia clínica) es para demostrar al paciente la atención recibida en caso de que el paciente haga el reclamo de un cobro que no corresponda. Se tiene acceso a todas las historias clínicas elaboradas durante la estancia del paciente, las recetas de farmacia, análisis, radiografías.

— *Módulo de Liquidación:* al ingresar a este módulo se genera el detalle de todos los costos incurridos en la atención médica del paciente. El desglose de la factura que se cobra al paciente puede ser total o parcial de acuerdo a las exigencias del mismo. La persona que tiene acceso a este perfil debe corroborar el costo total.

— *Módulo de Consulta Externa:* para ingresar a este módulo en el sistema se debe ingresar el usuario y contraseña del médico. En este módulo aparecen las citas que tiene el médico en el día, se pintan de diferente color las citas que ya han sido atendidas. En este módulo, el médico tiene una opción para señalar si el paciente no ha asistido a la consulta programada, esto le sirve como respaldo para demostrar que el médico está atendiendo en el horario establecido, el médico tiene que atender aproximadamente entre 20 a 24 fichas (pacientes). También en este módulo el médico puede bloquear el diagnóstico del paciente en caso de enfermedades que requieren mayor confidencialidad, por ejemplo VIH-SIDA, de tal manera que solo el médico tiene acceso al diagnóstico. En la historia clínica electrónica se tienen las vistas «tratamiento», «evolución» y «observaciones».

  El médico realiza la atención médica e ingresa el diagnóstico del paciente, una vez que guarda el diagnóstico en el sistema SISHAP, éste ya no puede ser modificado, por ejemplo al día siguiente, esta medida de seguridad es para evitar temas de negligencia médica o alguna mala praxis por parte del médico. Si puede realizar modificaciones a la historia clínica electrónica durante el tiempo establecido para la consulta, al día siguiente en su perfil le aparecerán las nuevas historias clínicas de los pacientes que debe atender en el día.

Cuando se hizo la presentación del sistema SISHAP en el auditorio, se reunió a todo el personal del Hospital Militar Central de COSSMIL: médicos, enfermeras y administrativos para conocer sus observaciones y/o sugerencias. También se mencionó que en la historia clínica electrónica, por seguridad al igual que en la historia clínica en papel, no se puede modificar la información de la misma (no se puede tachar, borrar, corregir con radex).

La historia clínica en soporte papel no puede tener registros como «ver sistema» o «tratamiento igual que el anterior»; para ello, en el Módulo de Consulta Externa se brinda la posibilidad que con un click puede repetir todo el diagnóstico anterior y el médico puede continuar con el nuevo diagnóstico.

La Dirección de Informática tiene claro que debe trabajar en el desarrollo de los módulos con otras áreas y/o unidades como Asesoría Jurídica, Unidad de Archivo Clínico, Jefes de Departamento y/o Servicio para tener un desarrollo consensuado y evitar el rechazo en su implementación. También es consciente de que la historia clínica en papel seguirá subsistiendo con la historia clínica electrónica.

8.3.3 SEGURO SOCIAL UNIVERSITARIO (SSU)

8.3.3.1 Seguro Social Universitario – Encargado de Bioestadística

Sector: Seguridad social	Nombre: Sr. Jaime Riveros
Institución: Seguro Social Universitario	Antigüedad: 31 años
Cargo: Encargado de Bioestadística	Fecha:10/09/2015

El Seguro Social Universitario (SSU) cuenta con expedientes clínicos manuales desde el año 1990 (en la actualidad estos expedientes se conservan como base de datos para el hospital); posteriormente, desde el año 2007, se ha implementado el Expediente Clínico Electrónico en Consulta Externa.

El Seguro Social Universitario prevé, para el Plan Operativo Anual (POA) 2016, desarrollar e implementar el expediente clínico electrónico en hospitalización. La actual Norma Técnica para el manejo del Expediente Clínico no menciona a los medios electrónicos, el Instituto Nacional de Seguros en Salud (INASES) debe trabajar en la aprobación de una normativa que reconozca el valor jurídico del expediente clínico electrónico.

El paciente en el Seguro Social Universitario puede recabar cita previa (ficha) en forma personal en el Hospital o mediante llamada telefónica; el SSU no cuenta con la opción de cita por Internet.

Dentro del Seguro Social Universitario, la historia clínica se maneja en dos Unidades:

— Unidad de Expediente Clínico, Archivo y Atención al Cliente.

— Unidad de Bioestadística.

8.3.3.1.1 *Unidad de Expediente Clínico, Archivo y Atención al Cliente*

Esta Unidad dentro del Seguro Social Universitario está encargada del expediente clínico único, es el único seguro que cuenta con un Expediente Clínico Único que consta de tres (3) partes:

a) *Consulta exte*rna: es la parte de evolución del paciente de forma cronológica, la misma es llenada por el médico.

b) *Auxiliares de diagnóstico y tratamie*nto: esta parte consta de las recetas médicas, análisis de laboratorios clínicos, informes que corresponden al paciente.

c) *Hospitalizaci*ón: desde el momento en el que el paciente ingresa al hospital se genera un expediente clínico único de hospitalización, donde se toma la presión, sus signos vitales; esta información se genera porque el paciente ingresa a emergencias. El médico de emergencias tiene que evaluar al paciente, extenderle una Hoja de Referencia que contiene los datos personales del paciente, la enfermedad por la que acude al hospital y un diagnóstico previo, con esta información se realiza la Admisión del Paciente.

Para que una persona pueda ingresar al Seguro Social Universitario, se realiza una evaluación pre ocupacional que consta de un examen psicológico, laboratorios y una radiografía de tórax.

Para la atención médica del paciente en el Seguro Social Universitario primero debe pasar por el médico generalista para que realice el primer diagnóstico y sea derivado al especialista.

La Consulta Externa cuenta con expediente clínico electrónico; el médico introduce el diagnóstico del paciente la prescripción de la receta, orden de laboratorio, radiografía y otros.

8.3.3.1.2 *Unidad de Bioestadística*

Está encarga del procesamiento de los datos bioestadísticos que se encuentran en el Expediente Clínico. Sin embargo, esta unidad aún

no ha implementado los datos estadísticos concernientes al expediente clínico electrónico implementado en Consulta Externa.

El formulario sobre la Codificación Internacional de Enfermedades (CIE 10) es un instrumento donde se encuentran todas las enfermedades existentes hasta la fecha, que llegan a ser aproximadamente 14.000 enfermedades definidas. Se tiene previsto que hasta el año 2018 se actualice el formulario CIE - 10 con la incorporación de 1.000 nuevas enfermedades existentes.

La Codificación Internacional de Enfermedades - CIE 10 ha sido creada para uniformar y unificar los diagnósticos de las enfermedades de todo el mundo, las mismas se distinguen de acuerdo a letras, números y en razón de las enfermedades con mayor índice de implicancia a nivel internacional. Esta codificación ha sido desarrollada por la Organización Mundial de la Salud (OMS) para fines epidemiológicos para comparar entre grupos, ciudades, pueblos, grupos etarios. El CIE - 10 se encuentra en su décima versión.

El trabajo de la Unidad de Bioestadística permite al Seguro Social Universitario determinar cuáles son las enfermedades más persistentes que son atendidas en el seguro, además de evaluar cuál es problema que genera este tipo de enfermedades.

En relación al Sistema Nacional de Información en Salud (SNIS) señala que éste ha sido creado para el área de la salud pública. La seguridad social tiene otras patologías diagnosticadas, por lo que mucha información requerida por el SNIS no puede ser enviada por el SSU.

El ente gestor de la información de la seguridad social es el Instituto Nacional de Seguros de Salud (INASES), entidad que está encargada de centralizar la información de la seguridad social, quiénes les brindan los parámetros para enviar la información, esto hace que se genere un conflicto entre ambas instancias SNIS e INASES. Hace un par de años ambas instituciones han tratado de unificar el manejo de la información en salud.

8.3.3.2 Seguro Social Universitario – Jefatura de Enfermería

Sector: Seguridad social	Nombre: Lic. Sonia Apaza
Institución: Seguro Social Universitario	Antigüedad: 21 años
Cargo: Jefe de Enfermeras a.i.	Fecha: 14/10/2015

El personal de enfermería del Seguro Social Universitario tiene conocimiento de la Norma Técnica para el manejo del Expediente clínico.

El Seguro Social Universitario maneja un expediente clínico que está dividido en tres (3) partes:

1. Consulta Externa: dentro de la misma se debe de considerar odontología y oftalmología.

2. Exámenes complementarios: internos o externos.

3. Hospitalización: que contempla un orden cronológico según las veces que se ha sido atendido el paciente.

El personal de enfermería es el encargado de abrir el expediente clínico del paciente, para lo cual solicita las tapas a la Unidad de Archivo, Admisión y Fichaje.

En el Seguro Social Universitario se ha intentado implementar el expediente clínico electrónico equipando a los consultorios con computadoras; pero desafortunadamente, este sistema no ha podido ser implementado debido a errores de impresión de la historia clínica (imprimía donde ya estaba escrito); como resultado, el SSU tuvo que volver a utilizar las máquinas de escribir para llenar las Hojas de Evolución, mismas que son llenadas por los internos[96] o médicos residentes[97] y revisadas y verificadas mediante V.º B.º por el médico tratante.

El personal de enfermería es responsable de realizar la verificación del llenado del expediente clínico; verifica que tenga los datos generales del paciente, que no falte ningún campo, que haya sido llenado correctamente por el médico residente y que tenga la firma y pie de firma del médico tratante.

Las enfermeras designadas a hospitalización (piso) revisan en detalle el expediente clínico para saber qué enfermedad tiene el paciente, cuáles son las indicaciones que dio el médico y qué medicamentos debe aplicar. En la consulta externa, la enfermera completa la historia clínica del paciente con los exámenes solicitados por el médico, por ejemplo, recoge los laboratorios, radiografías, tomografía y otros.

---

96 El interno es el estudiante de último año de medicina que realiza su año de internado rotatorio en un establecimiento de salud.

97 Médico residente es el médico que está haciendo su especialidad que dura tres (3) años.

Resulta problemático cuando la historia clínica no se encuentra en la Unidad de Archivo, Admisión y Fichaje, se encuentra extraviada en algún consultorio, en hospitalización, para investigación con un médico residente o trabajadora social; en esos casos se atiende al paciente y se abre una nueva historia.

En relación a la atención de los pacientes con VIH-SIDA, estos son atendidos como cualquier paciente, el SSU no los discrimina. Cuando el paciente es atendido quirúrgicamente el médico y personal sanitario toma las medidas de bioseguridad correspondientes (guantes, asepsia, otros). El paciente que tiene conocimiento de su enfermedad debe comunicarlo al personal sanitario para que tomen los recaudos correspondientes.

En relación al acceso, el paciente tiene derecho a acceder a su expediente clínico pero con la debida supervisión para evitar la mala interpretación en el momento de la lectura de su expediente, considerando que el diagnóstico del médico es presuntivo. El Seguro Social Universitario otorga al paciente la epicrisis[98], que es el resumen de la atención médica; se le brindará una determinada orientación para que no existan susceptibilidades del paciente que lo alarmen. Si el paciente desea acceder al expediente clínico completo, hará su solicitud mediante requerimiento fiscal u orden judicial.

Para la atención del paciente, el SSU cuenta con la Junta General de Médicos; los médicos especialistas hacen conocer la historia clínica de sus pacientes y en forma conjunta realizan el diagnóstico y tratamiento.

8.3.3.3 Seguro Social Universitario – Encargada de la Unidad de Admisión, Archivo y Fichaje

Sector: Seguridad social	Nombre: Lic. Elizabeth Saravia
Institución: Seguro Social Universitario	Antigüedad: 1 año
Cargo: Encargada de la Unidad de Admisión, Archivo y Fichaje	Fecha: 14/10/2015

[98] Constituye el resumen de todo el contenido del expediente clínico debe ser llenada en formularios expresamente diseñados…Asimismo, tiene carácter de informe resumido, motivo por el cual el médico tratante debe entregar una copia al paciente en el momento del alta, con énfasis en las indicaciones y/o recomendaciones que creyendo convenientes y que el paciente deba cumplir. Artículo 12 (Contenido específico), Norma Técnica para el manejo del Expediente Clínico.

8.3.3.3.1 *Protección de datos personales en el ámbito sanitario*

En el Seguro Social Universitario (SSU), cada componente del grupo familiar tiene su propio expediente clínico único, ordenado por fecha de nacimiento, diferenciado entre hombres y mujeres. Los hijos de los asegurados tienen acceso al seguro de salud hasta los veinticinco (25) años de edad, pasada esta edad, el SSU da de baja la historia clínica.

Los pacientes con VIH-SIDA, cuando tienen enfermedades comunes como ser resfriados, infecciones, otros, son atendidos en el SSU. Sin embargo, el personal del SSU no tiene conocimiento de qué paciente tiene VIH-SIDA; con el objetivo de no caer en temas de discriminación, las historias clínicas no tienen una codificación particular para estos casos.

8.3.3.3.2 *Historia Clínica (Expediente Clínico)*

Todas las personas que requieren atención del Seguro Social Universitario deben, de manera obligatoria, ser atendidos primero por el médico general. Realizado el diagnóstico, este médico deriva al paciente al médico especialista. La excepción se da únicamente con las mujeres embarazadas, quienes pueden dirigirse directamente al ginecólogo o emergencias.

La Unidad de Admisión, Archivo y Fichaje cumple estrictamente la Norma Técnica para el manejo del Expediente Clínico.

Cuando un trabajador de la Universidad o las instituciones afiliadas al SSU solicitan una cita médica, la Unidad de Admisión, Archivo y Fichaje le apertura un expediente clínico con las divisiones correspondientes.

El expediente clínico consta de tres (3) partes, cada una con la división respectiva:

1. Consulta Externa.
2. Laboratorios y exámenes complementarios.
3. Hospitalización.

El personal que accede al expediente clínico son los médicos y las enfermeras de consulta externa, hospitalización o emergencias, con la finalidad de evaluar al paciente.

En la Consulta Externa los médicos llenan, en el sistema, la historia clínica en formato electrónico. El sistema se denomina Gema 1 y Gema 2:

— Gema 1: reporte general del historial del paciente.

— Gema 2: la implementación de un mejor mecanismo de atención para el paciente, por ejemplo, en el registro de la agenda para la atención de los pacientes. Se dieron casos del registro de dos (2) pacientes en el mismo horario, todas estas dificultades han sido subsanadas por Gema 2, hay mejor orden y coordinación en la agenda.

La Unidad de Admisión, Archivo y Fichaje también tiene acceso al sistema, pero está restringido el acceso al diagnóstico del médico.

La enfermera es la encargada de realizar la solicitud de las historias clínicas a la Unidad de Admisión, Archivo y Fichaje, entregando 24 horas antes de la consulta el total de las solicitudes de atención (fichas) para que la Unidad realice la búsqueda de las historias clínicas en el Archivo. La enfermera, conforme el horario establecido (turno mañana o tarde), recoge las historias clínicas de la Unidad de Admisión, Archivo y Fichaje, para lo cual la Unidad de Admisión, mediante un listado de verificación, entrega las historias clínicas. Concluida la consulta externa u hospitalización, las enfermeras deben devolver las historias clínicas a la Unidad de Admisión, Archivo y Fichaje, registrando su devolución con nombre y firma de la enfermera.

Hay casos en los que la historia clínica de un determinado paciente no retorna a la Unidad de Admisión, Archivo y Fichaje, generalmente cuando hay cirugías ambulatorias (por ejemplo, aplicación de abastín en los ojos), debido a que el médico se olvidó de firmar la historia cuando atendió al paciente, en esos casos la Encargada de Archivo realiza la búsqueda en último lugar donde requirieron la historia clínica.

Si el paciente requiere su expediente clínico para tener una segunda opinión con un médico que no pertenece al seguro o con un médico del exterior del país, éste debe enviar una nota formal al Gerente de Salud solicitando el acceso a la historia clínica. El SSU facilita al

asegurado una fotocopia de los análisis, fotografía de la radiografía o informe del médico especialista que requiere. Para acceder al expediente clínico completo, el asegurado debe hacer su solicitud mediante requerimiento fiscal u orden judicial, en ese caso el SSU entregará una fotocopia legalizada y foliada conforme establece el procedimiento de la Norma Técnica para el manejo del expediente clínico, este tipo de solicitud del expediente clínico se presenta cuando el paciente considera que ha existido negligencia médica.

Las trabajadoras sociales del SSU también tienen acceso al expediente clínico del paciente, porque apoyan a los asegurados que no logran cubrir el total del monto de una cirugía o tratamiento. Asimismo, el expediente clínico puede ser solicitado por Auditoria Médica cuando existen requerimientos judiciales en casos de negligencia médica.

La Norma Técnica para el manejo del Expediente Clínico establece que el establecimiento de salud debe guardar la historia clínica por cinco (5) años. La Unidad de Admisión, Archivo y Fichaje realiza, cada tres (3) meses, la depuración de las historias clínicas de personas fallecidas, hijos de los asegurados titulares que hayan cumplido 25 años, historias que tienen más de 5 años. En los casos de hijos de asegurados titulares que hayan cumplido 25 años, el SSU no destruye las historias clínicas, las da de baja y se separan por si el hijo del asegurado se acoge al seguro voluntario del SSU.

8.3.3.3.3 *Seguridad de la información*

En la Unidad de Admisión, Archivo y Fichaje del Seguro Social Universitario trabajan cinco (5) personas que cubren los diferentes turnos que comienzan desde las 6:00 a.m. hasta las 21:00 p.m., después de esta hora la Unidad se cierra.

Esta situación se ha generado porque muchos de los médicos internistas (que hacen su internado rotatorio) o médicos residentes entraban por la noche a la Unidad y retiraban, con fines de investigación, expedientes clínicos; a raíz de esta situación los expedientes se perdían, razón por la cual la Gerencia de Salud del SSU ordena el cierre de la Unidad a las 21:00 p.m. Solo en casos de emergencia, las enfermeras o auxiliares de enfermería pueden retirar por la noche los expedientes clínicos, quienes al día siguiente informarán a la Encar-

gada o personal de la Unidad de Admisión, Archivo y Fichaje qué expedientes clínicos fueron retirados y dónde se encuentran (emergencias u hospitalización).

Hoy en día, para acceder al expediente clínico, los que hacen internado rotatorio y los médicos residentes deben solicitar el expediente a la Encargada de la Unidad para que les preste, en el día, los expedientes. Como mecanismo de respaldo, si alguno de ellos requiere retirar de la Unidad un expediente, se anotará en un cuaderno la fecha, hora, matrícula y nombre de quien hace la solicitud.

En el Seguro Social Universitario existe videovigilancia las 24 horas del día.

8.4 **SECTOR PRIVADO**

8.4.1 HOSPITAL ARCO IRIS

8.4.1.1 **Hospital Arco Iris – Dirección de Enseñanza e Investigación**

Sector: Privado sin fines de lucro	**Nombre: Dr. Igor Salvatierra**
Institución: Hospital Arco Iris	Antigüedad:
Cargo: Adjunto de Investigación	Fecha: 01/09/2015

8.4.1.1.1 *Hospital Arco Iris*

El Hospital Arco Iris (HAI) es un hospital de segundo nivel dentro de la categoría otorgada por el Ministerio de Salud; pertenece a la Fundación «Arco Iris», institución privada sin fines de lucro, fundada el 27 de septiembre de 2001; abrió sus puertas a la atención en noviembre del mismo año. El hospital fue construido por iniciativa del R.P. José Neunhofer con la finalidad de romper las barreras de exclusión económica y social, permitiendo la atención médica a la población en general de las ciudades de La Paz y El Alto; pero principalmente niños y niñas de la calle y personas de extrema pobreza hasta los 18 años de edad.

Se tienen estrategias para llegar a esta población a través ambulancias móviles que van a toda la ciudad mediante un cronograma planificado. Sin embargo, la necesidad de sustentar este servicio a los más necesitados impulsó a que se abra la atención de consulta externa a toda la población mediante el uso de una atención privada que genera recursos económicos.

A pesar de ser un Hospital privado, por convenio con el Ministerio de Salud, asume atenciones públicas como ser el Sistema Integral de Salud (SIS) que atiende gratuitamente a niños menores de 5 años y a mujeres gestantes en etapa prenatal, durante el parto y el seguimiento posparto hasta los seis (6) meses. El Estado, a través del Ministerio de Salud, realiza el reembolso de los gastos generados por esta atención conforme a los mismos costos que los hospitales públicos.

Todos los esfuerzos para otorgar una mejor atención a los pacientes se traducen en la incorporación de tecnologías dentro del sistema que maneja el HAI como un acto más humano en favor de los más necesitados.

Aproximadamente cuenta con trescientos (300) miembros dentro del hospital en todas las áreas, de los cuales un 30% es personal médico, 40% es personal de enfermería y lo restante es personal administrativo, mantenimiento y otros. Existen dieciséis (16) consultorios con treinta y cinco (35) especialidades, mediante los cuales se atiende aproximadamente entre trescientos (300) a cuatrocientos (400) pacientes diariamente.

8.4.1.1.2 *Historia Clínica (Expediente Clínico)*

La Historia Clínica es la herramienta fundamental con la que se hace el manejo institucional de la información del paciente. Ésta es individualizada, pero coadyuva a enfocar el colectivo de pacientes que llegan al Hospital; es decir, cada una de las historias clínicas representa una atención, medicación, un costo de consulta, una valoración para el área administrativa - financiera para conocer el costo la atención médica específica. Esta es una visión más administrativa y no muy médica pero que le da un plus a la historia clínica.

Dentro del Hospital, se tuvo una previa experiencia sobre el manejo de historias clínicas electrónicas a través del Internado Rotatorio del Hospital mediante herramientas ofimáticas (planillas en *Word*, tablas en *Excel*, base de datos en *Access*) que permitían agilizar el trabajo realizado en papel, pero mediante medios informáticos.

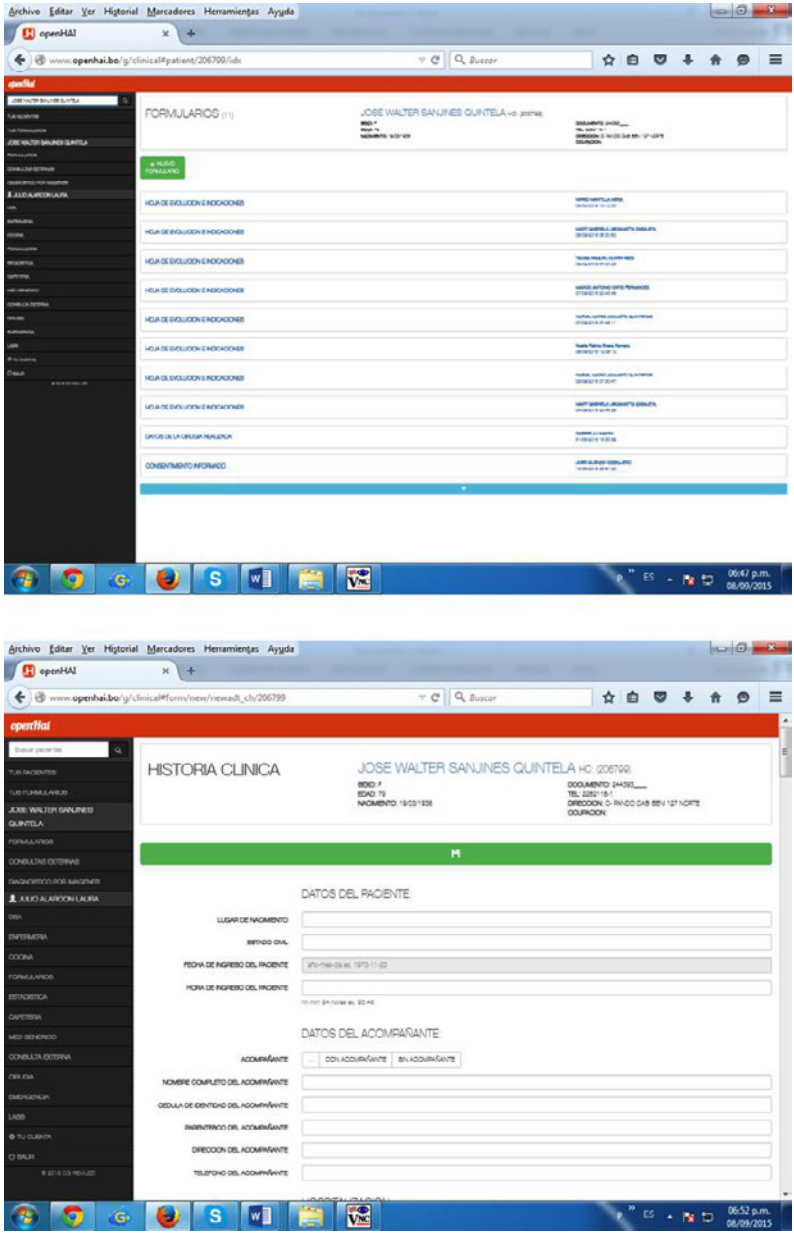

Figura 25. Vistas del módulo Historia Clínica Electrónica openHAI

Fuente de elaboración: Hospital Arco Iris.

Desde el año 2014 se tiene el sistema *openHAI* que funciona como una herramienta informática que permite organizar mejor, no solo la presentación física de la Historia Clínica, sino la generación de datos suficientes para la parte administrativo-financiera a fin de que se pueda organizar la atención dentro del hospital.

El sistema está diseñado en forma *on-line* y puede ser accedida desde cualquier lugar que tenga acceso a Internet. Contiene todos los formularios que normalmente se hace en papel. Por lo que se puede tener los datos generales del paciente de manera instantánea y a partir de estos datos se generan formularios específicos.

Estos formularios contienen: los datos de la enfermedad específica del paciente, el diagnóstico, los exámenes complementarios, las indicaciones médicas y también se tienen los informes del grupo de enfermería (registro de signos vitales, administración y vigilancia de fármacos, eventos acaecidos en la internación, etc.)

El diseño y la actualización del sistema *openHAI* son manejados por diferentes grupos de trabajo, los cuales son conformados por especialistas en informática y médicos especialistas por áreas.

Cada Historia Clínica esta modificada de acuerdo a las necesidades del paciente; es decir, que existe una HC para el recién nacido, otra para la atención ginecoobstetra, otra para la atención del adulto mayor, otra para gastroenterología y así para cada una de las especialidades. Aunque hay varios formularios, a todo este cuerpo se lo denomina Historia Clínica. En el pasado se lo hacía en papel, sin embargo, ahora lo realizan en forma digital y se centraliza en una base de datos.

Aún no se la denomina historia clínica electrónica porque en Bolivia, a la fecha, no se tienen los elementos suficientes para convertir esa historia clínica electrónica en una historia clínica con valor legal, porque ninguno de los miembros del HAI cuenta con una firma digital para dar solidez legal a este documento.

En este sentido, todos los formularios que son llenados de forma digital, para dar cumplimiento a la Ley 3131, son impresos, firmados y sellados de forma manual para que de esa manera tenga valor legal, convirtiéndose en un híbrido del pasado (Historia Clínica en papel)

con un instrumento actual (el sistema de la Historia Clínica Electrónica) que coadyuva con la obtención de datos que posteriormente pueden ser manejados en beneficio de la toma de decisiones dentro de la institución.

El tener un sistema que maneje las historias clínicas ayuda a tener un análisis periódico, permite un análisis epidemiológico de las atenciones, permite planificar mejor (cantidad de fármacos, camas necesarias para internación y otros).

Sin embargo, las limitaciones de la implementación de este sistema son: el temor a la innovación por parte del equipo médico, rechazo abierto o rechazo solapado al sistema no solo por parte de los médicos más antiguos sino también por parte de los médicos de menor edad. Existen algunos problemas en el sistema debido a la permanente actualización del mismo o por problemas eléctricos. También hay que tomar en cuenta los limitados recursos económicos destinados a la adquisición de soporte físico para la utilización del sistema, no todos los consultorios cuentan con un computador y una impresora. Normalmente el personal médico que trae su propia computadora es quien utiliza el sistema en la consulta externa.

Se realiza una capacitación en el uso de este sistema, no solo a los especialistas que hacen uso de esta tecnología, sino que a todo el personal que tiene interacción con la Historia Clínica. Estas capacitaciones son grupales y también individualizadas.

Actualmente todos los miembros del Hospital, mediante un instructivo, están obligados a utilizar el sistema *openHAI* de manejo de la historia clínica.

La historia clínica electrónica está completamente implementada en el Área de Hospitalización, con los médicos de guardia y los médicos de emergencias, pero aún se encuentra en etapa de prueba para Consulta Externa. Todavía no se conoce cuándo estará completamente implementada la historia clínica electrónica en todas las áreas del hospital, ya que esto depende de la asignación de recursos económicos que se destinen a la adquisición de hardware.

La utilización del sistema *openHAI* garantiza el manejo de la información para generar indicadores que ayudan a la organiza-

ción del Hospital, pero no garantiza la efectividad del acto médico. Cada personal médico es responsable de la calidad de información que ingresa al sistema, el mejor ejercicio del acto médico dependerá del conocimiento médico de cada usuario. El sistema no garantiza la calidad de la información ingresada, sino que hasta la verificación que se realiza posteriormente; recién en ese momento se puede verificar que lo ingresado en la historia clínica es lo adecuado para el paciente.

La historia clínica electrónica cuenta con varias partes como ser: los datos otorgados por el paciente, las preguntas realizadas por el médico y los resultados de los exámenes realizados por el médico al paciente. Ésta se elabora cada vez que existe una hospitalización.

La utilización del sistema *openHAI* ha permitido planificar una mejor atención a los pacientes, pero no permite evaluar si lo que el paciente recibe es lo adecuado para mejorar su salud. La calidad de la atención no se mide conforme a la cantidad de atenciones, sino a los resultados que se pueda tener de manera global y sostenible en el tiempo para todos los pacientes que han solicitado atención.

Es por eso que se hace tan necesaria la verificación después de haber llenado los formularios de la historia clínica electrónica y esto se lo hace a través de la impresión, el sello y la firma manual en el formulario impreso. Ahí se tiene la identificación de la conformidad del médico con todo lo que ha llenado en el sistema y se obliga a que el médico lea lo que ha escrito en el formulario ya que estampará su firma dando valor legal a ese documento y por ende generará responsabilidad por su contenido.

Como una evaluación preliminar de la implementación de la historia clínica electrónica, se tiene que hay gran aceptación por parte del personal, un manejo creciente especialmente por parte del área de enfermería.

8.4.1.1.3 *Seguridad de la Información*

La historia clínica tiene características propias de seguridad para saber quién se ocupa de ésta. Se tienen cuentas electrónicas mediante un identificador de usuario y una contraseña que permiten identificar

a la persona que ingresa a la historia clínica, ya que esto permite responsabilizar al usuario sobre el manejo de la historia clínica. Las cuentas son otorgadas a todo el equipo médico (especialistas, médicos de guardia, médicos de emergencias) y también los médicos que están realizando su internado rotatorio.

Cada una de las personas que tienen sus cuentas electrónicas es responsable de la información introducida en la historia clínica. Sin embargo, cada usuario después de ingresar al sistema toda la información, solo adquiere valor legal cuando se imprime, selle y firme el formulario que genere la historia clínica.

Otra forma de proteger los sistemas de información es la generación de energía eléctrica ante eventuales cortes del suministro eléctrico. El hospital cuenta con generadores eléctricos que se activan cuando existe un corte y los puntos críticos que gozan de este beneficio son: quirófano, terapia intermedia e intensiva y los servidores del sistema *openHAI*.

Dentro del sistema *openHAI* existe la otorgación de privilegios mediante los perfiles de usuarios de acuerdo con las características de cada uno. Cada persona que ingresa al sistema solo tendrá acceso a los formularios que están relacionados a sus labores dentro del Hospital.

Todos los ingresos al sistema y las modificaciones en el mismo son registrados a fin de crear un vínculo de responsabilidad sobre el llenado de los formularios de la historia clínica.

Una vez que se ingresa al sistema *openHAI,* el usuario puede ver toda la historia clínica y esto es un beneficio global a todos los usuarios. Pero solo visualizarlo no puede modificar a menos que sea el área que tiene permitido modificar de acuerdo a su especialidad o tarea dentro del hospital. Independientemente de la especialidad se puede visualizar los formularios llenados por cualquier otra especialidad con el fin de conocer el estado del paciente y tener un panorama claro de la situación de salud que tiene.

El sistema *openHAI* tiene la opción del autograbado; sin embargo, antes de imprimir, el mismo sistema verifica que todos los datos necesarios han sido llenados correctamente.

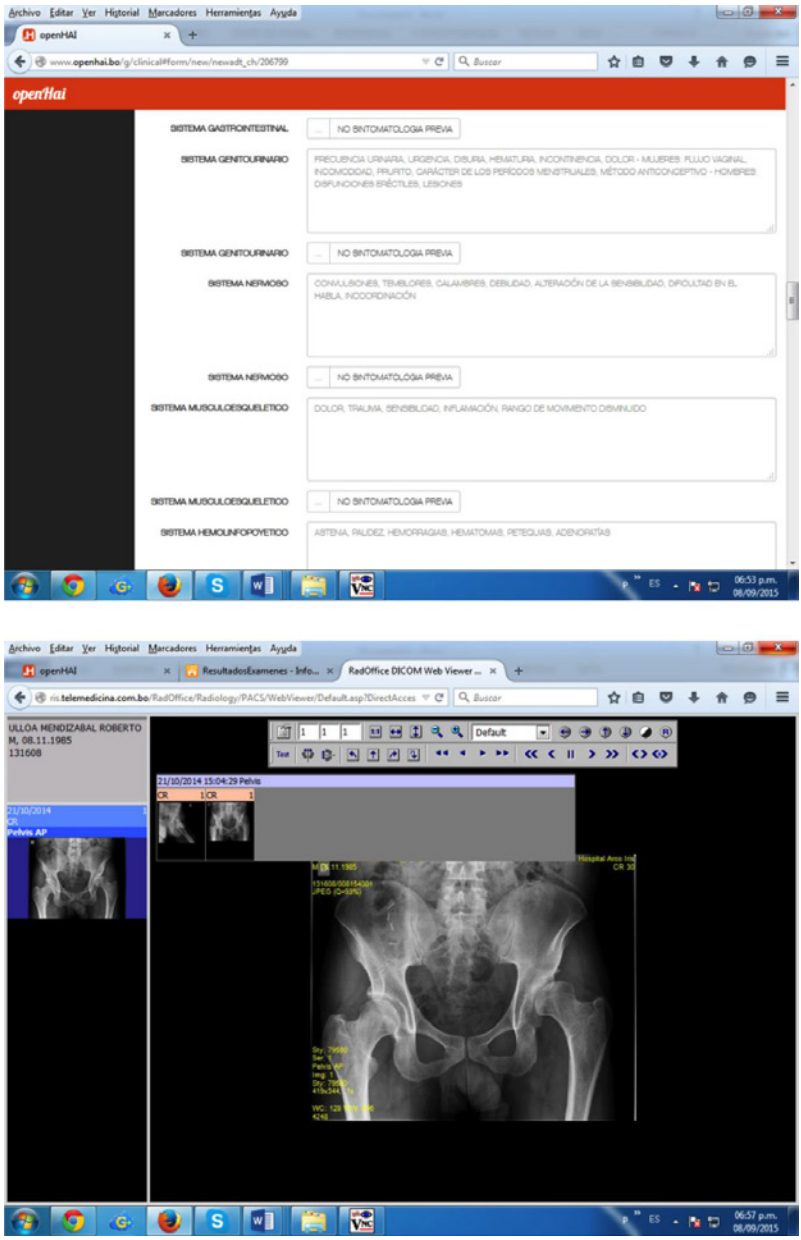

Figura 26. Vistas del módulo Historia Clínica Electrónica del openHAI

Fuente de elaboración: Hospital Arco Iris.

En el caso de que exista algún error en el llenado de la historia clínica, el sistema permite modificar los formularios pero para poder hacerlo, se debe llenar nuevamente el campo que estaba errado y el sistema exige un justificativo de la modificación de manera obligatoria. Este cambio se lo registra en la Hoja de Evolución del paciente que tiene todos los formularios de las historias clínicas. El tiempo otorgado para la modificación de los datos contenidos en la historia clínica, ha tenido una evolución. Para datos de historia clínica se tiene un plazo perentorio de 24 horas, mientras que las evoluciones específicas tienen un grabado automático, pero que puede ser objeto de modificaciones con la Hoja de Evolución para aclaraciones.

Todas las historias clínicas son pasibles a una auditoria médica por varias razones. Los casos difíciles, los casos de pacientes con prolongación de su estadía interhospitalaria, los casos de fallecimientos y algunos casos al azar son analizados por la Auditoria Médica.

Otra medida de seguridad de las historias clínicas es que no se puede modificar un formulario que no ha sido llenado por el mismo usuario, solamente el usuario puede modificar su contenido y esta modificación se registra en el mismo sistema.

No existe forma de que la historia clínica, sea en papel o electrónica, no contenga errores; es más, el hecho de que se generen errores permite realizar mejorías y, por consiguiente, existen avances para una mejor atención médica futura.

La capacitación sobre la utilización del sistema *openHAI* la realiza tanto el personal informático como también el personal de enseñanza médica.

8.4.1.1.4 *Otros datos importantes*

Según la experiencia que se tiene, el manejo de la Historia Clínica Electrónica en Estados Unidos se realiza mediante el sistema EPIC a través del cual se puede tener el historial de todos los datos de salud de un paciente durante toda su vida. Lamentablemente esto llega a ser tan voluminoso que muchas veces se hace complicado su manejo por problemas técnicos de transmisión de datos mediante la red.

En nuestro medio, se debería tener una mirada crítica hacia la implementación de la historia clínica electrónica ya que lamentablemen-

te en Bolivia no se cuenta con recursos tecnológicos y económicos como en los países más desarrollados. Pero se debe adecuar la utilización de esta importante herramienta a la realidad boliviana. No por seguir la tendencia mundial a migrar a esta tecnología se dejará a un lado la integración de los distintos modelos para obtener una historia clínica electrónica conforme a la realidad boliviana y que coadyuve a mejorar la atención a toda la población.

8.4.1.2 Hospital Arco Iris – Departamento de Tecnologías de Información

Sector: Privado sin fines de lucro	Nombre: Ing. Julio Alarcón
Institución: Hospital Arco Iris	Antigüedad:
Cargo: Jefe de la Unidad de Sistemas	Fecha: 04/08/2015 - 07/08/2015

8.4.1.2.1 *Sistema de Información Open HAI*

El Hospital Arco Iris (HAI) es un establecimiento de salud de tipo híbrido; es decir, que es público y al mismo tiempo privado, lo que implica que tiene otro tipo de formularios y otro tipo de tratamiento de pacientes. En consecuencia todo lo que desarrolla el Departamento Informático se basa en la norma boliviana; es decir, que sistematiza lo que la norma indica mediante el Ministerio de Salud. Actualmente se está emprendiendo el reto de facilitarle al médico el acceso al expediente clínico electrónico. La solución que el *openHAI* está desarrollando en estos últimos dos (2) años podría indicarse que ha satisfecho el 50% de lo que la norma prescribe, se realizan los formularios básicos del expediente, pero los médicos exigen más una vez que acceden a esta plataforma.

En base a lo que el gobierno boliviano ha establecido, el sistema hospitalario del HAI está diseñado en una plataforma *Open Source*, al mismo tiempo la base de datos es *Free Couch*DB realizado con asesoramiento italiano. La novedad del sistema es que el médico puede acceder al expediente clínico electrónico, desde dentro del Hospital como desde fuera de la institución. Además el sistema es multiplataforma; es

decir, que se puede acceder al expediente clínico electrónico desde cualquier dispositivo (*smartphone*, *tablet*, computadora portátil o *smart*TV) que tenga conexión a internet y tenga instalado un navegador web (Mozzilla, Google Chrome, Internet Explorer, Netscape y otros).

Una vez implementado el sistema en el HAI, éste ha sido bien aceptado a nivel de interfaz de usuario y cuenta con facilidades de impresión; de esta manera, mediante el sistema se realiza el expediente clínico y al final se debe imprimir la historia clínica con el fin de proceder a la firma manuscrita, esto debido a que en Bolivia lastimosamente aún no se cuenta con la firma electrónica[99].

Además de estas facilidades, el HAI ha instalado un servidor de impresoras mediante el cual, una vez que el médico ha registrado todos los datos en el expediente clínico electrónico, éste puede enviar a imprimir a cualquier impresora que esté conectada al servidor y que físicamente se encuentran en varios puntos estratégicos del hospital, sin la necesidad de estar en una computadora de escritorio, sin dependencia de un controlador específico sino solo con estar conectado a una red Wi-Fi; esto ha colaborado para la aceptación por parte del personal médico.

Toda la información que está almacenada en el sistema del HAI se encuentra en la nube. En el caso de una caída del internet, cuando se pretende acceder externamente es necesario contar con un Proveedor de Servicio de Internet (ISP); sin embargo, para ingresar internamente se tiene la intranet donde se puede acceder sin inconveniente.

El Hospital Arco Iris aceptó de manera positiva el sistema, ya que además de ser una institución híbrida como ya se mencionó, es también un hospital de enseñanza. Al año se tienen más de treinta y cinco (35) internos y cinco (5) residentes, siendo gente joven en formación, personas que son nativos digitales, para ellos no es difícil utilizar y trabajar con estos medios.

Existe, en el servicio sanitario, un Jefe de Sistemas. Además que los profesionales informáticos reciben capacitaciones a través de cursos a distancia, autocapacitación y capacitación interna. Dentro de las políticas del Departamento de Tecnología de Información (DTI) se esta-

---

[99] Este tipo de afirmación es frecuente en muchos entrevistados que desconocen la vigencia de la Ley 164 y su Decreto Supremo N.º 1793 Reglamento de la Ley 164 que otorga el valor jurídico probatorio de la firma digital.

blece que todo el personal debe saber de todo, no existe ningún secreto dentro del DTI; es importante contar con toda la información.

En cuanto al nivel de conocimiento en tecnologías de información y comunicación por parte del personal médico, se podría advertir que el hospital, al ser una institución joven con tan solo catorce (14) años de servicio a la sociedad, cuenta con personal joven en su mayoría, profesionales que están entre los veinticinco (25), treinta y cuarenta (40) años, por lo que se puede decir que el nivel de conocimiento en el manejo informático es bastante bueno.

Dentro de las políticas del DTI, el hospital cuenta con un servidor dedicado a proporcionar servicio de internet que permite administrar el ancho de banda. Todo el personal y los pacientes tienen acceso a Internet. Se cuenta con una red estructurada y una red inalámbrica. La distribución del ancho de banda se realiza mediante asignación de niveles de usuario, por ejemplo, los gerentes tienen más acceso al ancho de banda. Cada uno de los usuarios que accede al Internet cuenta con un ID, es decir, que se controla la navegación en el buen sentido; éticamente no se ven las navegaciones, pero si existe alguna irregularidad se interviene, se tiene conocimiento sobre qué navegaciones ha tenido el usuario.

El personal tiene acceso al correo institucional; sin embargo, existe una lista negra de sitios no académicos o clínicos que están restringidos. En el caso del paciente, éste tiene acceso al Wi-Fi para que pueda realizar la navegación, ingresar al *whatsapp*; pero está restringido el acceso a *Facebook*.

El sistema informático hospitalario HAI Administrativo es el que controla los pagos, las cuentas por cobrar, fichaje, la facturación y otros asuntos administrativos. Es el homólogo del SIAF del sector público, mientras que el HIS sería el homólogo del SICE del sector público.

El Módulo de Dispensación de Medicamento genera la receta médica y va directamente a Farmacia a fin de que se le otorgue los medicamentos necesarios.

El Módulo de Emergencias tiene muchas bondades como ser un llenado más rápido y a través de *checklist* tiene reportes de pacientes en espera, informa sobre la cantidad de pacientes que aún no fueron derivados a otra Unidad para que pueda decidir si los internará, los dará de alta o los derivará a alguna otra especialidad.

El Módulo de Fichaje está relacionado con la parte clínica, por lo que el médico lo único que hace es registrar los datos en el expediente clínico del que ya el paciente fue registrado previamente cuando solicitó la ficha de atención. La solicitud de ficha puede realizarse por internet.

El módulo de receta farmacológica ha sido alimentado por varios productos, tanto genéricos como especiales, cada médico tiene su industria farmacológica favorita y el sistema debe poseer todos los nombres de un mismo medicamento, de tal manera que al generar la receta pueda prescribir el medicamento indicado, la dosificación prescrita y otras indicaciones para la toma de fármacos.

Todos los formularios que son llenados por el médico tienen una estructura necesariamente técnico-médica ya que se deben cumplir con los estándares de salud establecidos.

Dentro del sistema también se pueden pedir estudios complementarios: análisis de laboratorio, examen de sangre, examen de orina, resonancia magnética, rayos X y otros que permitan tener un diagnóstico preciso del paciente.

Como proyecto del HAI está realizar una reingeniería de la red para interconectarla a través de fibra óptica. Para pensar en una solución informática en hardware se debe pensar también en una arquitectura informática en la red, debido a que puede ralentizar todos los servicios prestados por el sistema surgiendo un efecto en contra de la optimización de los servicios. El grabado automático genera consumo de tráfico de red ya que el sistema se comunica constantemente al servidor. Por otra parte el HAI cuenta con un circuito de vigilancia interna y externa, existen alrededor de ciento cincuenta (150) cámaras internas en el hospital y todas se encuentran en la red.

Sobre la inversión en tecnología, hasta el momento ésta ha sido realizada por etapas aproximadamente de trescientos mil dólares (300.000 USD) durante los últimos siete (7) años.

El organigrama clínico del HAI está clasificado por unidades de gestión clínica. Cuenta con cinco (5) unidades clínicas que son:

— La Unidad Quirúrgica donde se encuentran todas las especialidades que operan: traumatología, cirugía general, cirugía plástica, etc.

— La Unidad de Medicina Clínica es donde se encuentran todas las especialidades que no operan, pero que hacen seguimiento clínico: medicina interna, neumología, dermatología, cardiología y otras.

— La Unidad de Gestión Clínica Materno Infantil que está netamente relacionada con el tratamiento de madre y niño: pediatría, ginecología, obstetricia y otros.

— La Unidad de Diagnóstico por Imagen que compete a lo que es laboratorio, imagenología, fisioterapia.

La Unidad de Hospitalización que se encuentra clasificada en cuidados mínimos, intermedios y terapia intensiva.

También se cuentan con otras unidades menores como la de los servicios ambulatorios, la de emergencias, la de extensión comunitaria que son pequeñas clínicas móviles que salen diariamente a dar servicio de salud gratuito a todas las personas de escasos recursos.

El HAI, al ser una institución híbrida (pública y privada) como se había mencionado anteriormente, debe manejar las políticas públicas del Estado que se refieren a la atención de pacientes del Seguro Integral de Salud (SIS), seguro subvencionado por el Estado, atendiendo gratuitamente como política pública a la madre, a niños menores de cinco (5) años, personas con discapacidad y adultos mayores de sesenta (60) años.

Dentro del proceso de registro de personas atendidas por el SIS, una de las debilidades es que se debe llenar un formulario manual sobre su atención médica. Se realizan todas las atenciones que se requieren en base a una cartera de servicios preestablecidos por el SIS, ya que este seguro no cubre algunos servicios. En este sentido se atiende al paciente y posteriormente se remite al Estado el descargo mediante formularios que son llenados manualmente para que se realice la cancelación correspondiente por la atención brindada.

Además de la atención de políticas públicas, se realizan atenciones gratuitas conforme a la misión del hospital que es atender a los niños en situación de calle, para esto se utilizan las clínicas móviles que se dirigen hasta los lugares donde se encuentra esta población.

Uno de los principios del hospital es que los pacientes que cuentan con dinero pagan por las atenciones médicas recibidas, los que cuentan con menos recursos económicos pagan menos y los que no tienen

para cancelar por las atenciones no pagan, por lo que existe un área social que realiza el respectivo seguimiento.

8.4.1.2.2 *Relación del Sistema Nacional de Información en Salud (SNIS) y el sector privado sin fines de lucro*

En cuanto al grado de desarrollo y aplicación de las tecnologías en el Sistema Nacional de Salud, se puede indicar que es regular. Existe un intento del Servicio Departamental de Salud (SEDES) a través del desarrollo de los sistemas SIAF y SICE. Se sugiere que el Estado debería mínimamente proporcionar conexión de fibra óptica entre todos los hospitales, por lo menos a nivel metropolitano, y concentrar la información en un *Data Center* Departamental.

En Bolivia, aún no se tiene un sistema único para el manejo del expediente clínico electrónico, se debería pensar en algo como la interconexión de todo el Sistema Nacional de Salud. Lamentablemente, en la actualidad se da más importancia a los indicadores de epidemiología con los sistemas del SNIS que de alguna manera es secundario porque los sistemas del SNIS se consolidan al mes de ocurrido todo. Al Estado no le servirá de nada lo registrado si una epidemia cunde los primeros días y estos datos llegan con un retraso de veinte (20) a treinta (30) días. Los sistemas deberían llenarse en línea, pensando así en un *Data Center* para que esta información sea provechosa para la toma de decisiones a nivel Ministerio de Salud. Se deben pensar en las soluciones Web que son las que deberían predominar para decisiones a futuro.

El HAI envía la información requerida por el SNIS; al ser una institución híbrida pertenece a la Red Norte Central de los hospitales públicos.

8.4.1.2.3 *Protección de datos personales en el ámbito sanitario*

Se puede decir que en informática no existe 100% de seguridad; pero a nivel confiabilidad de los datos, el HAI trabaja con personal profesional que otorga esa confianza en el manejo de los datos.

El mayor beneficiario con el Expediente Clínico Electrónico es el paciente ya que se almacenan de manera inmediata toda su información. El paciente no puede ingresar al sistema en línea, únicamente se

puede imprimir su Historia Clínica Electrónica previa solicitud y requerimiento fiscal. Dicha solicitud se manda al Director General del Hospital y él mismo la deriva al Área Legal para su análisis, remitiendo una orden para la reimpresión del expediente del paciente; en sí, la información es del paciente, solo que esta resguardada en los servidores de HAI.

Una vez que son llenados los formularios por el médico o los internos, existe una opción para poder imprimir dichos formularios de manera directa o a través de un sistema de *networking printer*. De manera que no es necesario contar con los programas de instalación de las impresoras para enviar una impresión, sino sencillamente contar con una impresora conectada a una red para poder enviar a imprimir los formularios. Lo único pendiente sería la firma en el documento para que éste cuente con validez probatoria; sin embargo, con la firma electrónica esta falencia se subsanaría. Cuando un paciente desea tener una segunda opinión respecto a su tratamiento, el sistema *openHAI* puede generar un archivo PDF con todo el expediente clínico.

A través de un *smartphone* se puede acceder al sistema *openHAI* para registrar nuevos datos simplemente con la conexión a internet. Cuando se asigna un nombre de usuario al personal médico, se realiza a través de un protocolo de reclutamiento de recursos humanos mediante el cual se capturan todos los datos personales y se le otorga los privilegios para el acceso al sistema. Asimismo, cuando un médico renuncia al hospital, se procede a realizar la cancelación de la cuenta del usuario, pero se mantienen todos los actuados del mismo, en el caso de que decida volver o que sea necesaria una auditoría médica.

8.4.1.2.4 *Historia Clínica (Expediente Clínico)*

Hace 2 años, el Hospital Arco Iris (HAI) emprendió el proyecto para sistematizar el expediente clínico electrónico. Dentro de lo normado por el Ministerio de Salud, el HAI cumple con los doce (12) formularios que un establecimiento de salud debería utilizar. Entre ellos están: la epicrisis, la historia clínica, la hoja de evolución, la nota de alta y otros formularios.

En Bolivia, a nivel de sistemas, se habla de tres tipos: Sistema Informático Hospitalario (HIS), Sistema de Almacenamiento de Imágenes Radiológicas (RIS) y los PACS.

El Sistema Informático Hospitalario (HIS) se resume en el expediente clínico electrónico. El Sistema de Almacenamiento de Imágenes Radiológicas (RIS) y el PACS son sistemas donde se almacenan las resonancias, tomografías, rayos X y cualquier otra imagen radiológica que pueda surgir.

El sistema también genera las pulseras de identificación. Cada paciente que ingresa al HAI, el sistema automáticamente le genera una aplicación con un código QR (en ingles *Quick Response Code*) a fin de que el especialista, en el caso de desconocer el nombre del paciente, a través de este código y de un lector QR, directamente desde su celular puede armar el expediente clínico del paciente, generando así una facilidad para la identificación de los pacientes.

El médico puede realizar dos tipos de seguimiento mediante el menú: «Tus pacientes» y «Tus formularios». En «Tus pacientes» se encuentran todos los pacientes que el médico y sus colegas están tratando, se puede acceder a toda la información que los especialistas informan sobre el mismo paciente. Puede ser que varios médicos estén tratando a un mismo paciente. El especialista que está haciendo seguimiento a un paciente, entrando a «Tus pacientes», ve todos los pacientes que él y un grupo de médicos están atendiendo para realizar el seguimiento. «Tus formularios» son todos los formularios que el especialista ha ido llenando en el expediente clínico electrónico. Puede ir agregando nuevos formularios conforme a lo que tenga que registrar en el expediente clínico o revisar los formularios que ya fueron llenados.

Se cuentan con todos los formularios que la norma de salud exige, además que también hay formularios propios del HAI que permiten tener un mejor registro de cada paciente. Todos los datos que son llenados en los formularios cuentan con un procedimiento de autograbado; es decir, una vez que se pasa de un campo a otro, el sistema automáticamente procede al grabado en la base de datos.

En el caso de corrección de la información previamente llenada, el creador del formulario tiene acceso a editar. Además de contar con campos que tienen datos de validación que permiten mitigar el ingreso de datos errados.

Todo formulario subido al sistema, además de los establecidos por la norma boliviana, son de creación de los Jefes de Servicio, consensuado por un Comité y asesorado además por dos (2) médicos especialistas que trabajan en el Área de Enseñanza que son los que dan los

aportes clínicos. En base a su experiencia desde su formación académica, hasta su ejercicio profesional teniendo en cuenta que en su mayoría los médicos realizan su especialidad fuera del país, éstos ven los sistemas informáticos de otros países, en base a esta experiencia asesoran en la construcción de nuevos formularios.

En primera instancia se crea un prototipo, el cual es puesto a consideración de los involucrados; es decir, el personal que va a llenar dicho formulario para que ellos vean el producto, aporten ideas y así poder mejorar el resultado final. El área de Sistemas también participa de estas reuniones, pero una vez que se consensuan con las partes intervinientes, recién empieza la producción y el desarrollo para evitar el rechazo en la inserción de un nuevo formulario. Todo este proceso conlleva un tiempo de demora, pero se piensa que dentro de un año aproximadamente este sistema será un software de referencia nacional.

La documentación, en cuanto a diccionario de datos, marco teórico, marco conceptual de la base de datos, diseño de la base de datos, todavía no está desarrollada de forma escrita; evidentemente esto es de conocimiento del personal del área, pero hasta ahora no se plasmó en un documento escrito.

8.4.1.2.5 *Seguridad de la Información*

El sistema cuenta con medidas de seguridad para su ingreso, es así que solo los médicos registrados en el dominio pueden acceder al expediente clínico electrónico. Para que un médico pueda ingresar debe estar registrando en el sitio web del HAI, además de pasar por dos validaciones. La primera validación se da cuando se verifica que el médico está registrado en el dominio, una vez que el Departamento de Recursos Humanos ha dado un aval para que el Departamento de Tecnologías de Información (DTI) realice el registro del médico en el dominio. La segunda validación es realizada por el sistema validando en el dominio a través del cual ingresa. Cada médico cuenta con un correo institucional y a través de este correo se realiza la validación, tanto en el servidor del correo institucional como en el servidor del gestor de base de datos. El Hospital tiene dos (2) URL o dos (2) direcciones, una dirección para ser utilizada en intranet y una dirección a nivel nube. Una vez que el médico ya es un usuario registrado puede acceder tanto a nivel LAN como a nivel externo.

Otra medida de seguridad es la que se utiliza mediante el registro *log*. Cada vez que un usuario ingresa, sale, agrega, elimina, modifica o realiza cualquier actividad en el sistema, es registrado y resguardado en un archivo *log*, de tal manera que si ocurriera un atentado, el DTI reporta el nombre de usuario y la hora en que sucedió dicho atentado. Por política institucional, no se apunta a la persona física, sino se señala el nombre de usuario con el que se ha querido realizar o se ha realizado el atentado.

El sistema cuenta con administración de niveles de usuarios. Cada usuario puede acceder a los módulos a los cuales se le ha asignado la autorización para acceder. Generalmente los médicos cirujanos son los que tienen más acceso ya que están en todas las etapas de la evolución del paciente. Los médicos que trabajan en Consulta Externa sólo tienen acceso a ese módulo.

El HAI cuenta con un generador de energía en sus áreas críticas. El sistema *openHAI*, el *Data Center*, los ascensores, los quirófanos están conectados al generador si existiera un corte de energía. El generador provee energía eléctrica suficiente para tres (3) días.

El Sistema HIS maneja el estándar HL7, porque a través de este protocolo se sincroniza el sistema HIS con el sistema RIS PACS, es decir, que el mensaje HL7 permite la integración, siendo el sistema RIS PACS de una empresa tercerizada ya que la misma vende el almacenamiento de imágenes, pero para poder comunicarse con ese sistema de almacenamiento de imágenes se utiliza el estándar HL7.

El estándar HL7 es un código interno que genera el HIS que hace que automáticamente se abra el expediente de estudios radiológicos. El sistema hospitalario informático se comunica con el sistema RIS PACS que es el sistema de almacenamiento de imágenes a través de este estándar que permite la integración de los sistemas clínicos.

En cuestión de seguridad de la información, el HAI maneja un concepto diferente además de los cortafuegos y los *back ups*. La parte más importante a ser resguardada es la información, siendo está reguardada en cuatro (4) niveles. El primer nivel es en el servidor de producción que cuenta con medidas acceso y seguridad. El segundo nivel es un servidor espejo (redundante), todo dato que se está registrando en el sistema Open HAI es grabado de forma automática en el servidor espejo, este servidor espejo se encuentra en el mismo *Data Center* en el HAI. El tercer nivel de seguridad es la protección de la

información a través de *back ups* diarios programados a media noche; se cuenta con un NAS (servidor nube) donde, a una hora programada, los *back ups* son generados automáticamente y son subidos a un servidor externo que no está ubicado en el *Data Center* del HAI. Por último, el cuarto nivel es el ejercicio de resguardar los *back ups* en la nube *(cloud computing)*. Actualmente el espacio utilizado por el sistema *openHAI* es un servicio gratuito con capacidad de quince (15) gigas de almacenamiento. Para pasar estas cuatro (4) barreras, la persona tendría que trabajar en el hospital y conocer todas las rutas, ya que un ataque externo podría llegar máximo hasta el segundo nivel, los otros dos (2) niveles son netamente de conocimiento interno del personal de la institución.

Como ya se había mencionado, la información contenida en los sistemas está guardada a cuatro (4) niveles, en caso de acontecer una caída fuerte y perjudicar a los dos (2) servidores, al de producción y al espejo, se puede tardar unas seis (6) horas para poder restablecer la conexión.

A parte de las medidas de seguridad que se tienen en los sistemas, también se cuenta con cámaras de seguridad y los monitores en la Unidad de Terapia Intensiva (UTI) que están conectadas al sistema a fin de salvaguardar la vida de los pacientes.

Existen tres (3) centrales de grabación de las cámaras de seguridad (DVR). Una central pública, que está registrada en el Ministerio de Trabajo porque existe una norma en contra del acoso laboral, conformada por treinta y dos (32) cámaras y mediante consenso entre los empleados se autorizó la grabación. También existen otras redes que son privadas, como la red de vigilancia clínica, red de emergencia, red en UTI, otra en los cubículos de emergencias. A estas redes privadas solo puede acceder personal autorizado, mediante un nombre de usuario y una contraseña. La implementación de cámaras de seguridad se realiza en base a una solicitud de la Unidad Administrativa quien es la responsable de las imágenes grabadas por las cámaras.

En cuanto al control de calidad, se tiene un área que trabaja al respecto; sin embargo, específicamente el software es controlado a nivel usuario. Son los mismos usuarios quienes retroalimentan las falencias que pueden existir en el sistema *openHAI*. Al ser un software de desarrollo propio, los usuarios manifiestan si un dato incorporado

es correcto o incorrecto y luego se procede a corregirlo, siendo al final un software a medida de sus necesidades.

En cuanto al uso de la firma electrónica, en el hospital está pensado en su implementación; sin embargo, la herramienta no está puesta en práctica ni validada, inicialmente porque no se tiene la prioridad desde el Estado que obligue a hacer esto; aunque, ya el software está listo para funcionar con firma electrónica.

Hay que tomar en cuenta que toda base de datos tiene archivos *log* donde se registran los eventos que realiza de cada usuario. En cuanto a la revisión de los *log,* como en la mayoría de las instituciones, se la realiza cuando ocurre un incidente fuerte, contando con toda esta información. Actualmente no se realiza auditoría informática al sistema HAI.

En cuanto al plan de seguridad el HAI, éste cuenta con toda la documentación del manejo de los sistemas, un manual de funciones, las funciones específicas de cada miembro del DTI, los procesos informáticos, el Plan Operativo Anual y otros documentos relevantes al Departamento.

8.5 ANÁLISIS DE LAS ENTREVISTAS

En este punto se desarrollarán las entrevistas realizadas en el subsector público al Sistema Nacional de Información en Salud (SNIS) y los sistemas de información que forman parte SOAPS, SICE Y SIAF.

Sector: Público	**Nombre: Dr. Rocco Abruzzese**
Institución: Sistema Nacional de Información en Salud	Antigüedad: 8 años
Cargo: Responsable Nacional de Información y Producción de Servicios del Primer Nivel	Fecha: 17/06/2015 - 24/06/2015

Sector: Público	**Nombre: Ing. Mauricio Bustillos**
Institución: Sistema Nacional de Información en Salud	Antigüedad:
Cargo: Responsable del Software de Atención Primaria en Salud (SOAPS)	Fecha: 23/07/2015

Sector: Público	Nombre: Ing. Gabriel Jiménez
Institución: Sistema Nacional de Información en Salud	Antigüedad:
Cargo: Responsable del Sistema de Información Clínica Estadística (SICE) y Sistema de Información Administrativa Financiera (SIAF)	Fecha: 03/08/2015 - 27/08/2015

Sistema Nacional de Información en Salud.

El SNIS ha sido creado en octubre de 1990 con el nombre de «Subsistema Nacional de Información en Salud - SNIS». A partir del año 2000, se introduce el SNIS de II generación y la introducción de la normativa funcional del ciclo de la información hasta ahora vigentes, los instrumentos de sistematización y los de consolidación con una mayor cantidad de variables, así como la consolidación del manejo de la vigilancia epidemiológica. A partir del año 2006, este avance es más notorio con la implementación de la tecnología a través de la plataforma de comunicaciones e introducción de las herramientas informáticas que coadyuvan a la sistematización de los datos.

El SNIS es la unidad responsable de proveer al país, y al sector salud, de datos e información para la gerencia y la vigilancia epidemiológica que permitan tomar decisiones adecuadas y oportunas en la planificación, ejecución y evaluación de políticas públicas en el ámbito de la salud.

Hasta el momento el SNIS realiza la parte estadística en lo referido a salud pública; en el ámbito privado, se entregan formularios de consolidación. El SNIS solamente recoge información de los establecimientos de salud pública y seguridad social a corto plazo, lamentablemente no solicita información de los establecimientos de salud privados y organismos con o sin fines de lucro.

El registro de los datos, en el ámbito de los establecimientos de salud del primer nivel es realizado casi en su totalidad por el auxiliar de enfermería y por el médico, en aquellos centros donde existe este recurso humano. El llenado de los instrumentos de sistematización lleva mucho tiempo por lo extenso que es en su contenido, existen muchos instrumentos (cuadernos, formularios e instructivos). La falta de permanencia del personal médico y de enfermería en el estableci-

miento de salud, particularmente en el área rural donde los profesionales nuevos realizan su año de provincia y luego son promovidos o sustituidos con un personal con menos conocimiento sobre la organización y funcionamiento del SNIS, genera problema a este respecto.

Se requiere un programa de capacitación continuo al personal del sector salud en el manejo, análisis y construcción de indicadores, así como también en los determinantes de la salud (educación y vivienda, servicios básicos y medio ambiente), con una metodología adecuada y con un fuerte componente en la parte práctica y particularmente en el llenado de los formularios de captura de datos básicos y su reporte oportuno al nivel inmediato superior en la estructura.

El sistema informático que se utiliza en el SNIS es obsoleto y retrasa el procesamiento de datos para su difusión según cronograma de entregas. Existe la urgente necesidad de sustituir los equipos con otros de mayor capacidad y velocidad (equipos de última generación), con el fin de cumplir oportunamente con su entrega y difusión a las autoridades del Ministerio de Salud y a los usuarios del entorno al sistema de información en salud.

Los sistemas con que cuenta el SNIS-VE son los siguientes:

— *Sistema de Atención Primaria en Salud (SOAPS):* Registra los antecedentes básicos de filiación de las personas que son atendidas en el servicio (datos socio-demográficos, Carnet de Vacunación, Carnet de Salud e Historia Clínica de cada paciente); asimismo, están relacionados con la atención a usuarios o clientes de un servicio, denominado consumo del servicio o bien físico.

  Cada establecimiento de salud cuenta con cuadernos generados por el SNIS, los cuales son elaborados en base a los programas del Ministerio de Salud, como ser: cuaderno de consulta externa, cuaderno de mujeres en estado de gestación, cuaderno de atención integral del menor de 5 años, cuaderno de anticoncepción, cuaderno de internación, cuaderno de odontología, cuaderno de actividades del establecimiento de salud con la comunidad, etc. El cuaderno no es una Historia Clínica, es un sistematizador.

  De todos estos cuadernos, se elaboró un software; el SOAPS. La aplicación del SOAPS prescinde definitivamente la utiliza-

ción de los cuadernos en los establecimientos, reduciendo al personal de salud del tiempo requerido para el llenado de estos registros administrativos, punto de inflexión para la automatización de los procesos de gestión de la información desde su sistematización en adelante.

Todavía los establecimientos de salud del área rural no cuentan con este software y aún llenan los cuadernos de manera manual, ello porque no cuentan con la infraestructura tecnológica necesaria. Actualmente el 65% de todos los establecimientos de salud está utilizando el sistema. Un 35% aún realiza el llenado de los cuadernos de forma manual.

Todo el sistema de consolidación pretende tener datos de morbilidad de las personas dentro del territorio nacional. Existe un aproximado de 25% de error debido a la transcripción de los datos por lo que existe un 75% de confiabilidad.

— *Sistema de Información de Clínico Estadístico (SICE):* Automatiza el proceso de admisión de pacientes, registro de datos de consulta externa, internación y servicios complementarios de hospitales de segundo y tercer nivel. Con el SICE se logra que la información clínica y estadística se registre en un solo lugar y esté almacenada para que pueda ser usada por el establecimiento, uno de los principales problemas de la información clínica y estadística es que se utilizan muchos tipos de registros y cada registro es solo propiedad del servicio que lo llena, evitando así que la información sea útil a toda la institución. El sistema permite tener la información clínica y estadística del establecimiento en línea, por ejemplo, en el momento en el que laboratorio emita y registre el resultado de un análisis, el médico de consulta externa puede ingresar desde su consultorio a dicho análisis.

Los principales procesos que apoya el SICE son: 1) Admisión de Consulta Externa, 2) Admisión Hospitalaria, 3) Archivo Clínico, 4) Registro de Consulta Externa desde el servicio de consulta externa y/o en estadística, 5) Registro de Emergencias, 6) Internaciones y altas hospitalarias, 7) Servicios auxiliares como Rayos X, Ecografía, Laboratorio, Mamografía, Nutrición, etc., 8) Registro de Hechos Vitales, 9) Impresión y generación de formularios de consolidación definidos por el SNIS, 10) Envío

de información de hechos vitales al sistema SIAHV, y 11) Generación de archivo desagregado atención por atención a plataforma web de consolidación del SNIS-VE.

En el SICE, cada usuario tiene su contraseña porque hay niveles de acceso o perfiles para el administrador, el médico, la enfermera, el estadístico. En caso de modificaciones el usuario entra con su código y puede modificar datos, porque no es historia clínica sino solamente un proceso. La enfermera es la que llena los antecedentes del paciente como edad, peso, talla; en función a esa información, el sistema calcula el estado nutricional automáticamente. Una vez llenados estos datos por la enfermera, el médico, desde su perfil, llenará el motivo de la consulta; es un campo libre en el cual se pueden escribir hasta 5.000 caracteres.

El Sistema de Administración Financiera (SIAF): Diseñado para la administración de hospitales bolivianos, tiene como objetivo trabajar e integrar los procesos administrativos y financieros de un establecimiento de salud, de modo que la información se pueda procesar de forma automática, confiable y oportuna; pueda apoyar a la administración, planificación, análisis y toma de decisiones preferentemente en los hospitales del subsector público. Este sistema integral además permite la administración de farmacias, almacenes, activos fijos, recursos humanos y contabilidad.

El SIAF no es una historia clínica, es un registro clínico donde se encuentra: 1) Información básica del paciente, 2) Información del diagnóstico del paciente, 3) Información básica del tratamiento. Utiliza la Codificación Internacional de Enfermedades denominado CIE 10; es un sistema que codifica, en base a reglas, el tipo de diagnóstico descriptivo que pueda realizar el médico, lo que hace posible un reporte de enfermedades existentes en nuestro país.

PARTE IV

CONCLUSIONES

CAPÍTULO IX
CONCLUSIONES

Como producto del análisis documental del estado del arte y las entrevistas realizadas a profesionales sanitarios (médicos, enfermeras, personal administrativo), profesionales en tecnologías de la información y comunicaciones (TIC) y pacientes, se realiza la contrastación de la hipótesis y los objetivos específicos propuestos (y) para finalmente arribar a las conclusiones de la presente investigación.

Posteriormente, se señalarán los trabajos derivados a que ha dado lugar y por último se fijará una serie de líneas de investigación derivadas de la presente investigación.

9.1 CON RELACIÓN A LOS OBJETIVOS ESPECÍFICOS

9.1.1 ANALIZAR LA ESTRUCTURA, FUNCIONAMIENTO Y LIMITACIONES DEL SISTEMA NACIONAL DE SALUD DE BOLIVIA

En el Capítulo I se analiza la estructura, funcionamiento y limitaciones del Sistema Nacional de Salud, por lo que este objetivo se considera alcanzado. Dentro de este análisis y por su importancia, se destacan las siguientes conclusiones:

— El sistema sanitario es la forma en que una sociedad organiza sus instituciones sanitarias y cómo moviliza sus recursos para financiar estas instituciones, constituyendo el principal escenario de la política sanitaria.

— En Bolivia el «Vivir Bien» es un concepto milenario sustentado por las cosmovisiones de los pueblos indígenas originarios, fuertemente vinculado a la relación armoniosa con la naturaleza y a un modo de realización humana desde una vivencia holística y comunitaria; constituye el fundamento del Plan Nacional de Desarrollo *«Bolivia Digna, Soberana, Productiva y Democrática para Vivir Bien»* y mayor reconocimiento en la Constitución Política del Estado Plurinacional. Las políticas de salud en Bolivia se enmarcan en los derechos y obligaciones

determinados por la Constitución Política del Estado Plurinacional (CPE) vigente desde el año 2009. En alineación con la Constitución y diferentes documentos estratégicos nacionales (Plan Nacional de Desarrollo, Planes de Gobierno, etc.), el Ministerio de Salud elaboró el Plan Sectorial de Desarrollo (PSD) que determina las políticas de salud del Estado para un periodo de cinco años (2011-2015).

— La Salud Familiar Comunitaria Intercultural (SAFCI) tiene el objetivo principal de garantizar la inclusión y acceso universal a la salud, reconociendo que este es un derecho político, social, económico, cultural y ambiental, de todas las bolivianas y todos los bolivianos, para quienes los problemas de salud se resolverán en la medida en que se tomen acciones sobre sus determinantes a partir de la corresponsabilidad de los actores en la toma de decisiones sobre la atención de salud mediante la gestión participativa en el marco de la reciprocidad y complementariedad con todas las medicinas.

— La segmentación del Sistema Nacional de Salud boliviano se da debido a que el mismo tiene tres (3) subsectores de salud que responden a distintas formas: de financiamiento, de organización, de prestaciones y que atienden a diferentes segmentos de la población: el subsector público, el subsector de la seguridad social y el subsector privado. El *subsector público*, encabezado por el Ministerio de Salud, está compuesto por el conjunto de instituciones, recursos y servicios de salud dependientes de las entidades territoriales del Estado Plurinacional, de la administración central y descentralizada (Gobiernos Municipales y Departamentales). Por otra parte, existen establecimientos de salud dependientes de las Fuerzas Armadas, Policía y de las Universidades Públicas que se consideran generalmente como pertenecientes al subsector público. El subsector público está financiado principalmente por recursos provenientes de la fiscalidad general, así como por recursos provenientes de la venta de servicios y recursos externos. El *subsector de la seguridad social* está compuesto por diferentes entidades estatales (Caja Nacional de Salud) o privadas (Caja de Salud de la Banca Privada) y es regulado por el Código de Seguridad Social. Su financiamiento proviene principalmente de los aportes de empleadores públicos y privados. El *subsector privado* incluye los

consultorios particulares, policonsultorios y clínicas con fines de lucro, además de proveedores sin fines de lucro de ONG e Iglesia. El financiamiento del subsector privado proviene principalmente de los pagos de bolsillo realizados por la población atendida, además de compra de servicios por parte de seguros privados, financiados por cotizaciones de empleadores privados o por cotizaciones individuales.

— Las políticas públicas en Bolivia también consideran un *subsector de la medicina tradicional*, este subsector se destaca por la forma de atención y los conocimientos utilizados (en oposición a la medicina académica), pero no por el modo de financiamiento u organización; desde este enfoque, la casi-totalidad de los proveedores de medicina tradicional y natural pertenecen al subsector privado.

— En Bolivia existen 3.747 establecimientos de salud; de éstos, el 92% corresponde al primer nivel de atención (puestos de salud y centros de salud), el 6,5% al segundo nivel (hospitales básicos) y el 1,5% al tercer nivel (hospitales generales e institutos especializados). De acuerdo con los datos oficiales, en Bolivia hay 1,1 camas de hospital por cada mil habitantes, por norma se debe contar con 2,5 camas por mil habitantes, indicador que muestra una brecha entre la infraestructura de salud y las necesidades de su población. Hay 250 hospitales de segundo nivel y debería haber 500; se tienen 34 hospitales de tercer nivel y en Bolivia se debería contar con al menos 80. Se debería tener 54.000 funcionarios en salud y actualmente se tiene 24.091. En la gestión 2014, el presupuesto total de salud fue de 12.007 mil millones de bolivianos (1.725 millones de dólares) que representa un gasto per cápita de 172 dólares, que es el más bajo de la región. En el otro extremo se encuentran Chile, que tiene 787 dólares, y Uruguay con 1.000 dólares per cápita.

— Los establecimientos de primer nivel se encuentran principalmente en el área rural mientras que los establecimientos de tercer nivel están concentrados en el área urbana. Las redes de servicios no poseen enlaces funcionales ni operativos. Lo señalado evidencia un funcionamiento desarticulado y no sistemático de los niveles central y departamental del Ministerio de Salud con los niveles municipales. Esta fragmentación provoca

duplicidad de procesos administrativos y la existencia de múltiples intermediarios, elevando los costos de transacción. Además, esto constituye un obstáculo en la conducción y regulación sanitaria, limitando la implementación de los programas y proyectos a nivel nacional.

— El Sistema Nacional de Información en Salud (SNIS) es la unidad responsable de proveer al país, y al sector salud de datos e información para la gerencia y la vigilancia epidemiológica que permitan tomar decisiones adecuadas y oportunas en la planificación, ejecución y evaluación de políticas públicas en el ámbito de la salud. Tres sistemas alimentan de información al SNIS: el Sistema de Atención Primaria en Salud (SOAPS), el Sistema de Información de Clínico Estadístico (SICE) y el Sistema de Administración Financiera (SIAF). El SOAPS es un desarrollo propio del Ministerio de Salud que recoge información de los establecimientos de primer nivel (puestos de salud y centros de salud), el SICE y el SIAF son softwares desarrollados y donados al Ministerio de Salud en 2005 por *Medicus Mundi*; recogen información de establecimientos de segundo nivel (hospitales básicos) y tercer nivel (hospitales generales e institutos especializados).

— La debilidad del SNIS es que dispone de información solo del subsector público; el subsector de seguridad social envía poca información y el subsector privado no envía información, razón por la cual no tiene la información a nivel nacional de las prestaciones de salud. Otro problema es que lleva mucho tiempo el llenado de los instrumentos de sistematización ya que existen muchos instrumentos (cuadernos, formularios e instructivos). Finalmente, la alta movilidad del personal médico y de enfermería en el establecimiento de salud, particularmente en el área rural, hace que se cuente con un personal con menos conocimiento sobre la organización y funcionamiento del SNIS.

— Finalmente, cabe señalar que el sistema de salud discrimina a la población entre privilegiados 30% y marginados 70% de la población. El 60% de esta exclusión está explicada por barreras externas al sistema, mientras que el 40% por barreras internas. Las principales barreras externas son el acceso a educación y agua, la calidad de la vivienda, el nivel económico, ser indíge-

na y vivir en el área rural. Por otra parte, las barreras internas son la dotación de recursos humanos e infraestructura, la cobertura de los servicios de vacunación y la cobertura de la seguridad social. El 80% del presupuesto en salud es gasto corriente y 20% inversión (equipos, medicamentos, insumos, otros).

9.1.2 ANALIZAR LA LEGISLACIÓN SOBRE EL TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO SANITARIO DE ESPAÑA Y BOLIVIA

En los Capítulos III y IV se ha procedido a analizar de forma exhaustiva la normativa en materia de protección de datos sanitarios existente tanto en España como en Bolivia, por lo que se ha conseguido este objetivo. Dentro de este análisis y por su importancia, destacamos las siguientes conclusiones:

— En el ámbito internacional hay una conciencia generalizada sobre la importancia y complejidad que encierran las prácticas de tratamiento de datos de salud, partiendo desde el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, sobre la protección de las personas en lo que respecta al tratamiento automatizado de sus datos de carácter personal; la Recomendación R(97)5, de 13 de febrero, relativa a la protección de datos médicos, que presta una atención especial a los datos genéticos; el Convenio relativo a los Derechos Humanos y la Biomedicina de 4 de abril de 1997 (también conocido como Convenio de Oviedo) que presta una especial atención a las cuestiones relativas al genoma humano; y la Directiva 95/46/CE de 24 de octubre, relativa a la protección de datos de las personas físicas en lo que respecta a su tratamiento y a la libre circulación de los mismos. Este recorrido realizado por la normativa comunitaria sobre protección de datos en el ámbito sanitario permite percibir una constante preocupación por la protección del derecho a la intimidad en el tratamiento de datos personales, prestándose una atención particular a los datos sanitarios por la especial sensibilidad conferida a los mismos.

— El Tribunal Constitucional español, en su Sentencia 292/2000 viene a definir el derecho a la protección de datos como aquel que tiene todo ciudadano de disponer libremente de sus datos

personales tanto frente al Estado como ante cualquier particular, desvinculándolo del derecho a la intimidad y configurándolo como un derecho fundamental independiente; de esta forma, se habla del derecho a la autodeterminación informativa y de la libertad informática como términos conceptuales que definen la verdadera naturaleza de la protección de datos personales.

— En España la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) viene a sustituir a la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), a la que deroga. Tiene por finalidad principal incorporar al derecho interno español la Directiva 95/46/CE. El ámbito de la LOPD abarca los datos de carácter personal registrados en soporte físico, no necesariamente ficheros informatizados, que los hace susceptibles de tratamiento y toda modalidad de uso posterior de los mismos por los sectores público y privado; como novedad incluye al derecho de oposición y se caracteriza por ser una normativa matizada por numerosas excepciones.

— Los datos médicos o de salud son un concepto muy amplio, comprende todos los datos que de alguna forma se refieran a la salud tanto de las personas con buena salud, como de las enfermas o fallecidas. La LOPD considera a los datos de salud como datos especialmente sensibles. La primera Sentencia Constitucional 0965/2004 de fecha 23 de junio de 2004 considera a los datos de salud como «información sensible». La legislación boliviana no define a qué se entiende por datos médicos o de salud.

— El cumplimiento de la información en la recogida de datos también puede tener excepciones en el ámbito sanitario, esta información podría llevarse cabo en el momento de la entrada en el sistema sanitario bajo diferentes formas, por ejemplo, en el momento de la obtención de la tarjeta individual sanitaria (TIS), pero sería de difícil implantación en cada uno de los actos sanitarios que se lleven a cabo con los pacientes. Lo que se quiere evitar es dificultar la gestión asistencial y que pierda el sentido, por lo que otra forma de dar esa información, como se viene haciendo en algunos centros y servicios sanitarios de España, es incluir una leyenda en el formulario de recogida de

datos que alerte a los pacientes sobre sus derechos en relación al tratamiento de sus datos personales, y hacerlo una vez al ingresar el paciente en el centro y que no se convierta en un acto reiterativo para cada acto asistencial.

— En relación al consentimiento del paciente, se puede decir que, en principio, juega un papel importante, pero este queda posteriormente desvirtuado por las situaciones excepcionales en que éste se obvia, tanto en atención al interés público (por ejemplo para el desarrollo de la investigación científica) como a otros particulares. Las excepciones que otorga la LOPD a solicitar el consentimiento pueden hacer perder el sentido de pedir el mismo y ocasionar una generalizada práctica arbitraria, al no fijarse de modo específico las causales en que las citadas excepciones pueden ser aplicadas.

— La legislación boliviana regula sobre el consentimiento informado en la Ley 3131 del Ejercicio Profesional Médico, Decreto Supremo 28562 que reglamenta la Ley 3131, Decreto Supremo 0451 que reglamenta las disposiciones contenidas en la Ley 3729 para la prevención del VIH-SIDA, la Resolución Administrativa 158/ 2005 que aprueba el Reglamento para la elaboración, manejo y archivo del expediente médico o clínico en las entidades de la Seguridad Social a Corto Plazo, la Resolución Ministerial 0071 que aprueba el Código de Ética y Deontología de Enfermería, la Resolución Ministerial 0090 que regula la Norma Técnica para el Expediente Clínico y Obtención de Consentimiento Informado y el Código de Ética y Deontología Médica. El consentimiento informado es una declaración de voluntad efectuada por el paciente, familiares de primer grado o su representante legal, el cual luego de recibir información suficiente con respecto a su enfermedad y al procedimiento o intervención quirúrgica que se le propone médicamente aconsejable como la más correcta para la solución, mitigación o rehabilitación de su problema de salud, decide dar su conformidad y someterse a tal procedimiento o intervención. Se establece que en situaciones donde el paciente no tiene capacidad de decidir sobre su persona, requiere intervención profesional médica y no cuenta con un familiar, pariente o responsable legal, la institución de salud asume la decisión terapéutica siguiendo las normas y protocolos vigentes.

— Es importante determinar quién es el responsable del fichero de historias clínicas o de datos sanitarios, porque es el obligado a declarar los ficheros, ante él se ejercitarán los derechos de acceso, rectificación y cancelación (bloqueo) y es también quien va a responder ante la posible infracción que se cometa en este ámbito. En este sentido la Ley 41/2002 aporta luces al establecer que la gestión de la historia clínica por los centros se realiza a través de la *Unidad de Admisión y Documentación Clínica*, encargada de integrar en un solo archivo las historias clínicas, estando bajo la dirección del centro sanitario la custodia de las mismas; por tanto, en los centros sanitarios corresponde al Gerente la responsabilidad del fichero de historias clínicas. En el caso de profesionales sanitarios que desarrollan su actividad de manera individual, son ellos los responsables de la gestión y de la custodia de la documentación asistencial que generan.

— En la legislación boliviana la Resolución Ministerial 0090/2008 que aprueba la Norma Técnica para el Expediente Clínico señala que respetando las particularidades técnicas de archivo de cada establecimiento de salud, los expedientes Clínicos los custodia la *Unidad de Archivo y Estadísticas* en un único archivo central con dos grandes divisiones: activo y pasivo.

— Con la reforma de la Constitución Política del Estado en 2004 se incluye el «Recurso de Habeas Data» que en la nueva Constitución Política del Estado Plurinacional de Bolivia promulgada en febrero de 2009 se denomina «Acción de Protección de Privacidad». Tanto el ex-Recurso de Hábeas Data como la Acción de Protección de Privacidad utilizaron durante 8 años (desde 2004 hasta julio de 2012) el procedimiento del Recurso de Amparo Constitucional, hoy Acción de Amparo Constitucional. Asimismo, se aplicaron los requisitos de admisión y las causales de improcedencia, así como los principios de subsidiariedad (agotar la vía administrativa o judicial correspondiente) e inmediatez (interponer la acción dentro del plazo de 6 meses) del Amparo Constitucional. Con la aprobación del nuevo Código Procesal Constitucional en julio de 2012, se otorga un procedimiento propio a la Acción de Protección de Privacidad.

9.1.3 EXPLICAR LAS VENTAJAS Y DESVENTAJAS QUE BRINDA LA HISTORIA CLÍNICA ELECTRÓNICA PARA EL TRATAMIENTO DE DATOS SANITARIOS

En el Capítulo V se ha procedido a analizar de forma exhaustiva el concepto, naturaleza, propiedad archivo, conservación y custodia y acceso de la historia clínica, y en el Capítulo VI se desarrollan los modelos de servicios de salud, características, recogida y presentación de datos, seguridad y confidencialidad, estándares, ventajas y desventajas de la historia clínica electrónica; por lo que este objetivo se considera cumplido. Dentro de este análisis y por su importancia, se destacan las siguientes conclusiones:

— La historia clínica se puede considerar como la biografía sanitaria del paciente. Existe consenso por parte de muchos autores en considerar la historia clínica como uno de los documentos médicos más complejos que existen, debido a la diversidad de personas y organismos que en un determinado momento pueden estar interesados en tener acceso a los datos en ella contenidos, lo que compromete la intimidad del paciente. No se debe olvidar que los bienes y valores que se relacionan a la historia clínica son de una importancia extraordinaria ya que están directamente relacionados con derechos fundamentales de la persona como el derecho a la intimidad, a la salud, a la libertad y a la confidencialidad.

— En Bolivia, el régimen legal de la historia clínica está establecido en la Ley 3131 del ejercicio profesional médico, el Decreto reglamentario de la Ley 3131 y la Resolución Ministerial 0090 que aprueban la Norma Técnica para el manejo del Expediente clínico y la Obtención del Consentimiento Informado. La Norma Técnica contiene la definición de historia clínica, qué información debe formar parte del expediente clínico, consentimiento informado, tipos de expediente clínico, acceso, archivo, custodia, usos del expediente clínico asistencial, administrativo, legal, docencia, otros. Esta normativa no menciona el soporte electrónico; sin embargo, existen algunos proyectos aislados en el Sistema Nacional de Salud boliviano que están implementando la historia clínica electrónica, por otra parte, el Ministerio de Salud, mediante Resolución Ministerial, ha obligado a los centros y servicios sanitarios de segundo y tercer

nivel del subsector salud pública a implantar el Sistema de Información Clínico Estadístico (SICE).

— La historia clínica en manos del paciente corre el riesgo a que éste realice interpretaciones equivocadas de los comentarios expuestos en ella, unas veces por desconocer la materia, otras por considerarlos ofensivos y otras por ser comprometidos para él. El médico incluye también anotaciones personales clínicas y terminologías que van desde los más estrictos tecnicismos a otras que no los son tanto, pero que le son útiles aunque podrían molestar al enfermo si las viese.

— Lo importante y que cabe resaltar, no es el derecho a la propiedad sobre la historia clínica, sino el derecho de acceso a la misma. Se puede concluir que la historia clínica debe existir y mantenerse en el establecimiento de salud (consecuencia de la obligación legal de su conservación y custodia), sin perjuicio de que el paciente, en virtud del derecho de acceso a la misma, pueda conocer el contenido de sus documentos e informes. Lo cual no implica que el paciente ostente la titularidad única, entendida como plena capacidad de disposición sobre la misma, ya que se confirma a la luz de los derechos de rectificación y cancelación de datos regulados por la Ley 15/1999 de Protección de Datos de Carácter Personal de España, que la historia clínica no es susceptible de la cancelación automática que contempla el artículo 4.5, es decir, el paciente no puede imponer por su propia voluntad la destrucción o eliminación de datos de su historia clínica y, en relación al derecho de rectificación y cancelación de determinados datos, sólo podrá ejercitarlo cuando aquellos resulten inexactos, incompletos o inadecuados.

— La historia clínica debe contar el proceso asistencial de manera coherente, desde que el paciente es ingresado (o visto por primera vez en consulta) hasta que es dado de alta. Durante el proceso deben quedar registrados los elementos que proporcionen información de todo lo que ha ocurrido, notas de ingreso, hojas de evolución, registro de pruebas complementarias, resultados de las mismas, documentos de consentimiento informado, informes de alta, etc. La historia clínica que reúna estas características no solo ayudará al proceso clínico asistencial, lo cual es su finalidad principal, sino que ayudará considerable-

mente a dar consistencia a la actuación clínica del médico si le sucede la circunstancia de verse involucrado en un proceso judicial. Es decir, la redacción de una historia clínica correcta y su plasmación documental permitiría reducir sensiblemente las reclamaciones por negligencias médicas.

— Una historia clínica en papel ofrece estas dificultades: desorden y falta de uniformidad de documentos; información ilegible; la información se puede alterar; inaccesibilidad por no estar en el centro sanitario; errores en el archivo; poca garantía de confidencialidad a pesar del control riguroso por parte del responsable de la misma; deterioro del soporte por accidentes (agua y fuego); dificultad de separar los datos de filiación de los clínicos, entre otros.

— La historia clínica electrónica tiene como características que es completa, integra todos los episodios asistenciales del paciente no importa dónde ni cuándo se hayan producido; es interoperable con otros sistemas como los departamentales, los clínico-administrativos, de gestión económico-financiera y de gestión del conocimiento; accesible en cualquier momento y lugar en que sea necesaria para atender al paciente con las limitaciones debidas a la legislación de protección de datos (caso de España); flexible, permite su utilización a los investigadores, planificadores y evaluadores de la calidad de los servicios entre otros; segura y confidencial, todos los accesos a la historia deben ser registrados y debe identificarse quien accede y qué información introduce o modifica.

— Hoy en día la implementación de la historia clínica electrónica es una necesidad, porque las personas se mueven cada vez más de un lugar a otro y a lo largo de su vida es vista por diferentes profesionales; como consecuencia de ello, tiene más de una historia clínica distribuida en archivos informáticos y en papel en varias localizaciones y con varios números de identificación.

— Es frecuente el acceso a la historia clínica electrónica de un paciente por diferentes departamentos de un mismo centro y por distintos profesionales, con distintas necesidades; por ello, el sistema informático deberá atribuir perfiles (médico, especialista, fisioterapeuta, enfermera de planta, técnico de laboratorio, administrativa, etc.) y diseñar la historia de forma que las per-

sonas puedan acceder a los apartados que sean necesarios para la función asistencial que desempeñan y se impida el acceso a aquellas partes de la historia clínica respecto de las que no estén autorizados. La historia clínica electrónica permite hacer frente a estas cuestiones de una forma más eficaz que la historia en papel. La clave para mantener la seguridad y confidencialidad de los datos de salud está en establecer perfiles de usuario.

— La utilización inapropiada de la autorización para acceder a determinada información esta fuera del alcance de las TIC, dependerá de las personas, de los profesionales sanitarios. El sistema de información debe otorgar las medidas de seguridad adecuadas para que personas extrañas al ámbito sanitario puedan acceder a las historias clínicas. Las razones de interés para acceder a este tipo de información pueden ser variadas; se considera que una de las principales es la económica.

— Una de las claves para la implementación de la historia clínica electrónica es que sirva de instrumento de trabajo para los médicos y demás personal sanitario; que facilite su trabajo, no lo complique; sin introducir actividades nuevas que no sean imprescindibles, esto evitará que se produzcan fracasos en la implementación de los sistemas de historias clínicas. En el diseño de la historia clínica deben participar personas que conozcan las tareas clínicas y los datos que son relevantes, los cambios que deban introducirse después son siempre muy caros; no debe estar orientado por razones históricas, normas arbitrarias y usos no clínicos, tampoco se debe orientar las soluciones informáticas hacia la explotación de datos para gestores y sino como instrumento para la práctica clínica. El diseño de la historia clínica debe permitir llevar a cabo la integración de información clínica, poder revisar la organización de los servicios y de los profesionales.

— La historia clínica electrónica ofrece ventajas adicionales frente a la historia clínica almacenada en soporte papel, pudiendo agruparse sus prestaciones en las siguientes funcionalidades: gestión de la información en salud, manejo de resultados, manejo de órdenes médicas, sistemas de soporte para la toma de decisiones, sistemas de comunicación electrónica y conectivi-

dad, soporte al paciente, procesos administrativos, sistemas de reportes y salud pública, y emisión de informes médicos.

— Para garantizar la seguridad y confidencialidad de la información clínica se debe resolver la visibilidad de la historia clínica electrónica, para lo cual se establecerán protocolos y guías de actuación. El sistema de información permitirá que todos los accesos a la historia queden registrados (utilización de *logs*), se pueda identificar quién accede, qué información introduce o modifica (firma electrónica), entre otros. Es importante resaltar que se debe llegar a un *equilibrio entre seguridad* y *disponibilidad*; un exceso de medidas para garantizar la confidencialidad de los datos puede colapsar los sistemas y comprometer el acceso a la información, de forma que se impida cumplir con la principal función de la historia clínica electrónica, que es la asistencial, y pierda el sentido todo el proceso, no se debe olvidar que el fin último es ofrecer una atención sanitaria con calidad y eficiencia.

— La *Historia de Salud Electrónica (HSE)* no es una aplicación informática única, sino el resultado de la integración e interacción de varias fuentes de información, incluida la historia clínica electrónica, que tiene como resultado un auténtico sistema de información de salud. La Historia de Salud está constituida por un conjunto de registros heterogéneos que con soportes clásicos serían posiblemente inmanejables. La historia de salud electrónica precisa de estándares que hagan posible la interoperabilidad de diferentes sistemas de información sanitaria. La historia de salud electrónica presenta indudables ventajas en la atención del paciente, en la docencia y en la investigación, pero también en la gestión y planificación sanitaria y de salud pública. Sin embargo, para que sea posible su existencia, se precisan mecanismos de identificación de las personas y el cumplimiento estricto de los mecanismos de seguridad, confidencialidad y disponibilidad, que por otra parte se exigen por las normas legales vigentes.

— Pensar en *interoperabilidad* es fundamental en la planificación de un sistema de información sanitario; alinear la administración y gestión de la información con los objetivos del sistema sanitario y sus usuarios es el factor clave para el éxito. La inte-

roperabilidad es un atributo de los sistemas de información informatizados, imprescindibles para la gestión moderna de los sistemas sanitarios. Tiene la particularidad que su correcta aplicación la hace invisible para los profesionales de la salud que usan dichos sistemas, pues permite que la información fluya entre las distintas aplicaciones y sistemas. Los beneficios de diseñar sistemas interoperables son infinitos e irrenunciables, y van desde la integración de los datos de los pacientes de manera que permitan la toma de decisiones más adecuada, hasta la distribución universal de la información, la obtención de estadísticas e indicadores en tiempo real y otras funciones. Además, posibilita que distintas aplicaciones y sistemas se mantengan en esta red de información sin tener que modificar sus estructuras.

— Uno de los beneficios más importantes de la *Historia Clínica Personal (HCP)* es el mayor acceso de los pacientes a una amplia gama de información de salud confiable, datos y conocimiento. Los sistemas de historias clínicas personales son más que simples repositorios estáticos para los datos del paciente; se combinan los datos, conocimientos y herramientas de software que ayudan a los pacientes a convertirse en participantes activos en su propio cuidado. Los pacientes pueden aprovechar el acceso a la información para mejorar su salud y la gestión de sus enfermedades. La información puede ser altamente personalizada para hacer que la HCP sea más útil. Pacientes con enfermedades crónicas serán capaces de realizar un seguimiento a sus enfermedades junto con sus proveedores de atención médica. Las ventajas que presenta la Historia Clínica Personal (HCP) son: la persona controla la HCP y el acceso a la misma; captura de todas las fuentes los registros de salud del paciente; es privada y segura; es accesible desde cualquier lugar; permite el intercambio de información entre los proveedores servicios de salud; y es transparente. Finalmente, múltiples actores como pacientes, proveedores de servicios de salud, empleadores, contribuyentes, gobiernos e instituciones de investigación, juegan un papel clave en el desarrollo de la tecnología de la Historia Clínica Personal.

— A medida que el *uso de las redes sociales* se haga parte de la vida profesional de los médicos, es importante tener en cuenta una serie de recaudos, principalmente en lo que respecta a la

relación médico-paciente o médico-familia, donde la confidencialidad de la información no debe ser comprometida para que no se afecte la confianza establecida en el consultorio. Es importante destacar que las redes sociales crean nuevos dilemas éticos acerca del manejo de la información personal en salud por parte de los pacientes, que pueden exponer y publicar sus problemas para buscar opiniones sobre cómo tratar su problema de salud y relatarlo abiertamente.

— Las redes *sociales* están sirviendo para cambiar la forma en que las personas interactúan y se comunican, y esto también sucede en todo lo relacionado con la salud. Cada vez más aplicaciones móviles para la salud están siendo integradas en estas redes sociales. Los teléfonos móviles se están convirtiendo en una plataforma cada vez más importante para las intervenciones en salud. En los últimos años, los investigadores han utilizado los teléfonos móviles como herramientas para fomentar la actividad física y una alimentación sana, para la monitorización de los síntomas de enfermedades crónicas como el asma, diabetes, hipertensión, corazón, enfermedad pulmonar obstructiva crónica, tuberculosis y VIH/SIDA, y para una serie de otros problemas de salud, enviando a los pacientes recordatorios acerca de sus próximas citas, medicamentos que deben consumir, entre otros. Cabe mencionar que la mayoría de las intervenciones de teléfonos móviles basadas en el seguimiento de la información de salud se centran sólo en captura de información sobre las actividades de salud y los estados que están directamente vinculados a los objetivos de salud de los individuos.

— Al asociar automáticamente la información capturada sobre actividades relevantes para la salud y los estados con la ubicación, hora del día, y otra información contenida en el teléfono, como por ejemplo, los eventos del calendario o correos electrónicos recientes y llamadas telefónicas, podría ser utilizado para alertar a las personas de actividades saludables y recursos locales pertinentes a la situación de su salud (por ejemplo, restaurantes cercanos que sirven comida sana o una sugerencia para llevar un paseo después de una larga reunión). Recientes desarrollos de dispositivos médicos sofisticados que interactúan con los teléfonos móviles, tales como *Sistema iPhoneECG de AliveCor* (www.alivecor.com) o *Mobius de Mobisante Smartphone*

(www.mobisante.com) sistema de ultrasonido, podría permitir consultas a base de teléfono para una gama de condiciones, lo que facilita en gran medida la atención de especialistas en las áreas de salud donde los recursos son insuficientes.

— Se rescata del *«Informe de cumplimiento de la LOPD en hospitales»* elaborado por la Agencia Española de Protección de Datos que el cumplimiento de la normativa española es alto en el conjunto de centros privados, alcanzándose niveles elevados en la mayoría de conceptos clave analizados: inscripción de ficheros (99%), inclusión de cláusulas informativas en los formularios de recogida de datos (94,5%), disponibilidad de procedimientos para atender el ejercicio de los derechos de acceso, rectificación, oposición y cancelación (97%) y en general, en la implantación de medidas de seguridad y su auditoría periódica. En promedio, el nivel de cumplimiento en los centros públicos es menor que en los centros privados con excepción de las comunidades de La Rioja y Murcia. Las áreas de mejora más importantes son la instalación de carteles informativos sobre el derecho a la protección datos, la revisión periódica del Documento de Seguridad, el registro de todos los accesos a la información, el archivo de las historias clínicas en dispositivos dotados de mecanismos que obstaculicen su apertura, así como la adopción de medidas de seguridad para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte. Es importante destacar que en el caso de los hospitales de titularidad pública, los indicadores varían significativamente según el aspecto y comunidad autónoma de que se trate. La implementación de la Historia Clínica Electrónica alcanza al 55% de los hospitales encuestados, siendo mayor en los centros públicos que en los privados (67% frente a 44%).

— La incorporación de las tecnologías de la información y las comunicaciones (TIC) por parte de los Servicios de Salud de las Comunidades Autónomas de España ha dotado, en los últimos años, a usuarios y profesionales de sistemas y aplicaciones que han facilitado a ambos colectivos el acceso a una información de calidad sobre la salud individual, al servicio de una atención sanitaria de calidad creciente. Hoy todas las Comunidades Autónomas sin excepción tienen sistemas de Historia Clínica Electrónica (HCE), Historia de Salud Electrónica (HSE) o His-

toria Clínica Digital (HCD), en fase de implantación casi completa en Atención Primaria. Este nivel de implantación es menor en Atención Especializada. España, de la gestión 2006 a 2012, ha hecho una inversión de 252 millones de euros para implementar las TIC en las 17 Comunidades autónomas en el marco del «*Programa Sanidad en Línea*» (Fases I y II). Durante la primera fase de Sanidad en Línea (2006-2009) han sido proyectos clave la dotación de infraestructuras y servicios a las Comunidades Autónomas, la sincronización de tarjetas sanitarias autonómicas con la Base de Datos de Población Protegida del SNS y la consolidación de un Nodo Neutro con alta disponibilidad. Durante la segunda fase del Programa (2009-2012) ha desarrollado proyectos TIC dentro de los siguientes ejes de actuación: 1) Proyecto de Historia Digital del SNS para el intercambio de información clínica entre Comunidades Autónomas a través del Nodo Central del SNS, 2) Intercambio de información asociada a las recetas electrónicas entre diferentes Comunidades Autónomas a través del Nodo Central del SNS, y 3) Proyectos autonómicos de historia clínica electrónica y receta electrónica de los Servicios de Salud. El objetivo final del «Programa Sanidad en Línea» es permitir el acceso a parte de la información clínica de los ciudadanos españoles, desde cualquier punto del Sistema Nacional de Salud utilizando como llave un sistema interoperable de Tarjeta Sanitaria que permite identificar al paciente de forma unívoca y acceder a su información clínica independientemente de dónde esté almacenada.

9.1.4 IDENTIFICAR LAS MEDIDAS DE SEGURIDAD QUE BRINDAN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC) PARA EL TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO SANITARIO

En el Capítulo VII se ha procedido a identificar las medidas de seguridad que brindan las tecnologías de información y comunicación para el tratamiento de datos personales en el ámbito sanitario como ser software seguro, TIC en seguridad de la información (cortafuegos, proxies, redundancia, copia de respaldo, control de acceso ló-

gico y físico, directorios, medios de autenticación, registros log, reserva, otros), firma electrónica y auditoria informática, por lo que este objetivo se considera cumplido. Dentro de este análisis y por su importancia, se destacan las siguientes conclusiones:

— El Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007) de España tiene como objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamientos, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos personales. En este Reglamento se establecen tres niveles de medidas de seguridad: básico, medio y alto, siendo correspondientes las medidas de nivel alto para los ficheros que contengan datos de salud. Para poder implantar estas medidas, especialmente las organizativas, y que sean conocidas por las personas que intervengan en el tratamiento, tienen que estar escritas y el Reglamento obliga a que estén recogidas en un Documento de Seguridad, el mismo que es de obligado cumplimiento para los centros y servicios sanitarios de España. Este Documento debe identificar al responsable del fichero, el encargado del tratamiento y al o los responsables de seguridad.

— La contrastación entre la documentación revisada permite afirmar que hoy en día se cuenta con tecnología para la seguridad de la información que cumple con los requerimientos de la LOPD y el Reglamento de desarrollo de la LOPD de España como: software y sistemas seguros; para la eliminación de vulnerabilidades cortafuegos y proxies; redundancia, que en el caso de un fallo, puede tardar minutos en reponer el servicio; las copias de seguridad *(back up)* para recuperar la información; el control de accesos lógico y físico, que da la capacidad de controlar y conocer quién y cuándo accede a la información, a un mensaje o a un servicio, los directorios como LDAP son la clave de cualquier sistema de control de accesos en entornos medianos y grandes; la autenticación que consiste en la comprobación de la identidad del actor; la utilización de *logs* en aplicaciones, sistemas operativos y elementos red para registrar el uso que se hace de ellos y los posibles errores en el sistema; el cifrado, la técnica de seguridad más popular, que convierte a un mensaje en inteligible y se necesitará una clave para descifrar el

mensaje (firma electrónica); la reserva; y el control de calidad para evaluar la efectividad del centro o servicio sanitario en el mantenimiento y mejora de seguridad (auditoría informática).

— En Bolivia la Norma Técnica para el manejo del Expediente Clínico establece las medidas de seguridad para el soporte papel, no hace mención al soporte electrónico. Sin embargo, los desarrollos aislados que se tiene de Historia Clínica Electrónica en el Sector de Seguridad Social, Caja de Salud de la Banca Privada (CSBP) y Corporación del Seguro Militar Social (COSSMIL) y del subsector privado, Hospital Arco Iris (HAI) tienen como medidas de seguridad: software y sistemas seguros, cortafuegos y *proxies*, redundancia (servidor espejo), copias de seguridad *(back up)* para recuperar la información, control de accesos lógico y físico (*password*, tarjetas inteligentes, videovigilancia, otros), perfiles de acceso (médico, enfermera, personal administrativo), autenticación, utilización de *logs* en aplicaciones, sistemas operativos y elementos red y reserva. Para mayor seguridad, el acceso a la historia clínica electrónica en la CSBP y COSSMIL solo se realiza en el establecimiento de salud (consulta externa, hospitalización, emergencias), en el caso del HAI el médico tiene acceso desde cualquier dispositivo móvil que tenga acceso a Internet (tabletas, teléfonos móviles, laptop).

— La firma electrónica o firma digital está regulada en España por la Ley 59/2003 y en Bolivia por la Ley 164 General de Telecomunicaciones, Tecnologías de la Información y Comunicación y su Decreto reglamentario; es otro de los mecanismos que van a garantizar la seguridad de la información porque reúne cuatro características particulares: autenticación (la identidad de quien ha escrito el mensaje), integridad (que el mensaje no ha sido modificado), no repudio (la persona que envía el mensaje no puede negar el envío) y confidencialidad (que la información no puede ser conocida por otros). La firma electrónica consiste básicamente en la aplicación de cifrado (algoritmos de encriptación a los datos); de esta forma, el mensaje sólo será reconocido por el destinatario que podrá comprobar la identidad del remitente, la integridad del documento, la autoría y autenticación, preservando al mismo tiempo la confidencialidad. Para certificar que esta firma electrónica pertenece a determinada persona se encuentra el prestador de servicios de

certificación o entidad certificadora autorizada (tercero de confianza) para lo cual emitirá un certificado electrónico o certificado digital incorporado a la firma.

— Cabe mencionar que en Bolivia la *firma digital* cuenta con el marco legal correspondiente con la aprobación de la Ley 164 General de Telecomunicaciones, Tecnologías de Información, Decreto Reglamentario y Resoluciones Administrativas Regulatorias (RAR) emitidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT). La Ley 164 establece que la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), bajo tuición de la Vicepresidencia del Estado, prestará el servicio de certificación para el sector público y la población en general a nivel nacional. La ADSIB cuenta con la Infraestructura de Clave Pública (PKI) para funcionar como una Entidad Certificadora. En pasados meses ha sido auditada por la ATT para verificar que cumple con los requisitos técnicos, económicos y legales establecidos en la Ley, sus reglamentos y resoluciones administrativas; está a la espera de la autorización oficial de la ATT para empezar a prestar servicios. En una primera etapa la ADSIB ha suscrito convenios interinstitucionales con entidades del sector público la Aduana Nacional, la Autoridad de Supervisión del Sistema Financiero (ASFI), Vicepresidencia del Estado Plurinacional y Empresa Azucarera San Buena Aventura (EASBA) para iniciar, como piloto, el servicio de certificación y firma digital.

— El *costo del Certificado Digital* y *el Token USB* o *Tarjeta Inteligente* que se constituye en el soporte del certificado y la firma digital pueden ser una barrera para la implementación de la firma digital en Bolivia. La ADSIB emitirá tres (3) tipos de certificados digitales con diferentes costos para personas naturales 180 Bs. (24,5[100] euros), personas jurídicas 370 Bs. (50.40 euros) y cargo público 450 Bs. (61,3 euros); estos precios no son definitivos, cuando la ADSIB empiece a prestar servicios comercialmente presentará los precios oficiales aprobados me-

[100] Tipo de cambio 1 boliviano = 1 euro 7,34 bolivianos. Banco Central de Bolivia (2015), *«Tipos de cambio»* [en línea]: https://www.bcb.gob.bo/?q=cotizaciones_tc [Consulta: 25/09/2015].

diante Resolución Administrativa Regulatoria de la ATT. La validez del contrato con ADSIB es de un (1) año prorrogable a dos (2) años para certificados digitales de personas naturales y jurídicas. Asimismo, el artículo 29 Decreto Reglamentario de la Ley 164 establece la vigencia de dos (2) años para los certificados de cargos públicos. El costo del *token* USB o la tarjeta inteligente será aproximadamente de 313 Bs. (43 euros); el *token* no será provisto por la ADSIB, el interesado en contratar el servicio deberá llevar a la ADSIB el dispositivo de su elección (*token* USB o tarjeta inteligente). El costo aproximado de un certificado digital para persona natural que incluye el *token* o tarjeta inteligente será aproximadamente de 493 Bs. (67 euros), precio bastante alto para la economía de un ciudadano boliviano, más aún cuando el salario mínimo nacional es de 1.656 Bs[101] (226 euros), lo cual puede generar una brecha en el acceso al servicio.

— La otra Entidad Certificadora en Bolivia es *ASOBAN*[102] que presta servicios desde el 2002; tiene dos (2) tipos de certificados, Certificado Digital Clase 2 para correo electrónico seguro que tiene un costo de 1.200 Bs. (163 euros) y si se adquiere más de 20 certificados el costo baja a 860 Bs. (117 euros) y Certificado Digital Clase 3 para personas jurídicas (servicio adquiri-

---

101 «El presidente Evo Morales promulgó ayer el Decreto Supremo 2346, que fija un incremento salarial del 8,5% para la gestión 2015, y que sube el salario mínimo nacional en 15%, con lo que éste llega ahora a 1.656 bolivianos». «Cuando llegamos al Gobierno, el salario mínimo era apenas 40 dólares y ahora es 240 dólares. Antes, el penúltimo de América Latina y ahora está en la mitad de todos los países de América Latina. Nuestro deseo es garantizar el crecimiento económico para garantizar la estabilidad económica y seguir mejorando los salarios», manifestó Morales, en el acto que se desarrolló en Palacio de Gobierno. Página Siete (2015), *«Decreta, 8,5% de incremento y el salario mínimo sube a 1.656»* [en línea]: http://www.paginasiete.bo/nacional/2015/5/2/decretan-85-incremento-salario-minimo-sube-1656-55315.html [Consulta: 25/09/2015].

102 La Asociación de Bancos Privados de Bolivia (ASOBAN) tiene como misión ser una organización representativa del sistema bancario reconocida por su confiabilidad y liderazgo, que contribuye a la integración entre asociados, mercados, comunidad y región latinoamericana. ASOBAN (2015), *«Misión»* [en línea]: http://www.asoban.bo/certificados/manuales [Consulta: 30/09/2015].

do por los entidades financieras para garantizar que el portal del banco es un sitio web seguro). El contrato tiene una vigencia de un (1) año, ASOBAN no cuenta con *token* USB o tarjeta inteligente, el software debe bajarlo directamente al dispositivo donde se vaya a firmar digitalmente.

— En el ámbito sanitario, la investigadora ha apoyado a la Caja de Salud de la Banca Privada (CSBP) para que tome contacto con la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) y la Asociación de Bancos Privados de Bolivia (ASOBAN), ambas Entidades Certificadoras, para que conozcan la viabilidad de implementar el Certificado y Firma digital en el Software Médico y Sistema Administrativo Médico (SAMI) que contiene la historia clínica electrónica. La CSBP está interesada en implementar la utilización de la firma digital empezando con los médicos de la Regional La Paz y, en base a la experiencia, ampliar al resto de las regionales.

— ASOBAN tiene una relación directa con la Caja de Salud de la Banca Privada (son parte del Directorio de la CSBP), ASOBAN puede ofrecer el servicio. Pero ASOBAN, pese a estar funcionando desde el año 2002 como Entidad Certificadora, no tiene por el momento interés en conseguir la autorización de funcionamiento de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) conforme establece el artículo 81 (Autoridad y atribuciones) de la Ley 164. ASOBAN se ampara en la misma Ley en el artículo 80 (Certificados emitidos por entidades extranjeras), pero para que sus certificados tengan la misma validez y eficacia jurídica deben ser reconocidos por una entidad certificadora autorizada nacional (como será dentro de poco la ADSIB), está última cobrará a ASOBAN por el servicio, con lo cual, si ASOBAN emite 300 certificados digitales para los médicos de la Caja de Salud de la Banca Privada, tendrá que destinar parte de su ganancia al pago de la validación de los certificados a una Entidad Certificadora Autorizada.

— El artículo 96 del Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007) de España se refiere a la *auditoría informática*, estableciendo que los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría

interna o externa, que verifique el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos (2) años. La auditoría examina evidencias, si se producen incumplimientos de las medidas y prácticas de seguridad detalladas en la normativa de seguridad. La clave de una auditoría sea interna o externa es la independencia, la evaluación se debe hacer contra algún patrón, en este caso será contra el Reglamento de la LOPD. Existen diferencias entre auditoría e inspección; la auditoría que exige el Reglamento de desarrollo de la LOPD frente a la inspección, que puede realizar una de las Agencias de Protección de Datos (estatal o autonómica). Se considera que se debe utilizar la auditoría informática cómo una herramienta para la protección de la información, en este caso para el adecuado tratamiento de los datos de salud contenidos en las bases de datos y sistemas de información de los centros y servicios sanitarios públicos.

— En el caso de Bolivia, al no existir una ley específica de protección de datos, no hay obligación en llevar cada dos (2) años *auditorías informáticas*. La Norma Técnica para el manejo del Expediente Clínico establece el requerimiento del expediente clínico para la auditoría médica externa conforme el Manual de Auditoría y Norma Técnica para su realización, la normativa del ámbito sanitario no menciona a la auditoría informática. Por lo antes expuesto, en las entrevistas realizadas a los funcionarios de la Caja de Salud de la Banca Privada, Corporación del Seguro Militar Social y Hospital Arco Iris para conocer la experiencia de la historia clínica electrónica han manifestado que no realizan auditorías informáticas para el adecuado tratamiento de los datos de salud contenidos en las bases de datos y sistemas de información.

— Existe consenso entre varios autores al determinar que un componente muy importante en el tema de seguridad, además, de la que pueda otorgar las TIC, es el *factor humano*. Muchas veces se ha dicho que la persona puede ser el mejor guardián y protector de información tan sensible como son los datos de salud; pero también puede constituir la peor amenaza cuando no aplica la política de seguridad del centro o servicio sanitario o establecimiento de salud o entran en conflicto otros intereses, como puede ser el económico. Es por esta razón que se considera que

deben estar implicados desde la alta dirección hasta cada uno de los participantes del proceso asistencial y el tratamiento de la información, es una de las claves para tener una eficaz gestión de la seguridad y confidencialidad.

— Otro programa a tomar en consideración es la formación en manejo de las Tecnologías de Información y Comunicación (TIC). La introducción de las TIC en la sanidad es una realidad y va a más, está modificando la forma en que los profesionales trabajan lo que hace que requieran dominio de las nuevas herramientas. Es necesario intensificar la formación en las nuevas tecnologías que manejan los profesionales sanitarios con cursos básicos de informática (paquetes ofimáticos, Internet, uso de correo electrónico), de las aplicaciones, infraestructuras, innovaciones tecnológicas, entre otros, que les permita adquirir nuevas destrezas y conocimientos, esta formación coadyuvará a que se evite el rechazo y prejuicios a la innovación, quizás fundados más por desconocimiento y falta de domino de las TIC. En el caso particular del tratamiento de datos de salud, los profesionales sanitarios al conocer bien el funcionamiento de la herramienta con la que trabajan se convencerán que los datos de sus pacientes contenidos en las historias clínicas electrónicas están más seguros y pueden mantener la confidencialidad que requiere la legislación.

— Los servicios de cómputo en la nube *(cloud computing)* presentan retos al sistema jurídico nacional, internacional y por ello se propone partir de un marco claro y transparente en el ámbito contractual donde empresas y Gobierno se comprometan a lograr los mejores resultados y cumplir con los derechos que están en juego respecto de la información del mismo Estado y de los habitantes y/o ciudadanos. El que ofrece la contratación de *cloud computing* es un prestador de servicios que en la Ley de Protección de Datos de España tiene la calificación de «encargado del tratamiento». El cliente que contrata servicios de *cloud computing* sigue siendo responsable del tratamiento de los datos, por lo que la normativa aplicable al cliente y al prestador del servicio es la legislación española sobre protección de datos (Ley Orgánica 15/1999 y Reglamento de desarrollo – RLOPD). La aplicación de la legislación española no puede modificarse contractualmente. Finalmente, aunque le in-

formen que los datos personales están disociados, no cambia la ley aplicable ni la responsabilidad del cliente y del prestador del servicio. Las variantes en la modalidad de cómputo en la nube y los diferentes actores requieren certeza jurídica en regulación de los servicios de tratamiento, almacenamiento de información y otras capacidades de los recursos tecnológicos ligados a la nube. Se considera que los retos más relevantes para el éxito en términos de la adecuada adopción y desarrollo del cómputo en la nube son: privacidad, seguridad, confidencialidad y protección de datos personales, propiedad intelectual y jurisdicción aplicable.

— El *Big Data* o Datos Masivos promete grandes beneficios para la mejora de la salud de las personas, así como posibilidades nunca vistas para la toma de decisiones de gran trascendencia en salud pública, investigación, gestión de recursos sanitarios, etc., pero como contrapartida, también supone una intromisión sin precedente en la privacidad de los datos de salud de las personas. Se debe revisar las garantías y salvaguardias que deben adoptarse para conseguir que el *Big Data* Sanitario despliegue toda su potencia y proporcione todos los beneficios y avances científicos que se anuncian sin vaciar de contenido los derechos fundamentales de las personas y, en particular, su derecho fundamental a la protección de sus datos personales, eliminando o, al menos, mitigando en la medida de lo posible, los riesgos que aparecen en estos procesos.

9.1.5 EVALUAR EL ESTADO DE SITUACIÓN DE LA HISTORIA CLÍNICA E HISTORIA CLÍNICA ELECTRÓNICA EN LOS ESTABLECIMIENTOS DE SALUD DEL SISTEMA NACIONAL DE SALUD DE BOLIVIA

En el Capítulo VIII se ha procedido a evaluar el estado de situación de la historia clínica e historia clínica electrónica en los establecimientos de salud del Sistema Nacional de Salud de Bolivia y en particular de la ciudad de La Paz para lo cual se realizan veinticinco (25) entrevistas no estructuradas a funcionarios del subsector público (Ministerio de Salud, Sistema Nacional de Información en Salud),

subsector de la seguridad social (Caja de Salud de la Banca Privada, Corporación del Seguro Social Militar, Seguro Social Universitario), subsector privado sin fines de lucro (Hospital Arco Iris), por lo que este objetivo se ha conseguido. Dentro de este análisis y por su importancia, se destacan las siguientes conclusiones:

— Este Sistema Único de Información de Salud (SUIS) es una propuesta de la actual Ministra de Salud cuya implementación está considerada realizarse hasta la gestión 2020; el objetivo del SUIS es tener una plataforma virtual única en la que se otorgue un código a una persona, que estará inmerso dentro de la Cédula de Identidad. La nueva Historia Clínica Digital del SUIS debe ser desarrollada desde la visión del médico, que es la persona que está en contacto con el paciente y no desde el punto de vista del informático, que hace el desarrollo; esto en consecuencia de la implementación de sistemas de información en salud que son más estadísticos y administrativos que clínicos como es el caso del SOAPS, SICE y SIAF. Para el análisis, diseño e implementación del SUIS y la historia clínica digital se considera la experiencia de otros establecimientos de salud de Bolivia y otros países, también se ha solicitado el apoyo financiero a diversas organizaciones e instituciones internacionales como el Banco Interamericano del Desarrollo (BID), Agencia Española de Cooperación Internacional (AECID), FOREDES de Bélgica, Organización Panamericana de la Salud (OPS).

— La *Caja de Salud de la Banca Privada (CSBP)* tiene 17 años de servicio a su población asegurada. Desde la gestión 2005, los profesionales de la CSBP han desarrollado su propio Software Médico y Sistema Administrativo Médico (SAMI), el cual se aplica y utiliza actualmente en los Servicios de Consulta Externa (Policonsultorio) y Hospitalización a nivel nacional. El Sistema SAMI está constituido por veintiún (21) módulos médico administrativos, que interactúan entre sí e incluyen diversas áreas. El SAMI tiene un sistema configurable de usuarios y contraseñas con distintos niveles de acceso para cada profesional de la CSBP (médico, enfermera, administrativo, farmacia, laboratorio, etc.), de esta manera se asegura la confidencialidad, privacidad y seguridad de la información de cada paciente, los datos de los pacientes no pueden ser modificados y revelados a

terceros. Este sistema médico integra de manera sencilla las áreas de agendas médicas y el expediente clínico electrónico.

— La *Historia Clínica Electrónica del SAMI* cuenta con funciones y aplicaciones propias, contiene la información completa del Expediente Clínico de cada paciente, de forma cronológica, con fecha y hora de atención, permite clasificarlo de acuerdo al Régimen de Seguro y Programa de Salud, otorgarle órdenes de laboratorio, exámenes auxiliares, prescripciones médicas, órdenes de interconsulta, bajas médicas, certificado prenatal, entre muchos otros documentos. Además, puede obtener informes médicos, informes de junta médica, reportes de estudios comparativos entre la gama de variables con que cuenta el SAMI y reportes de seguimiento a la calidad del registro de la información. Con el SAMI se puede realizar una variedad de análisis estadísticos, investigaciones médicas, detección de factores de riesgo más frecuentes en la población asegurada, patologías prevalentes y todo tipo de reportes que sirven para elaborar planes de promoción y prevención, en la perspectiva de que un Sistema de Salud es más eficaz en la medida en que prevenga la aparición de enfermedades más que tenga un enfoque curativo y asistencialista.

— En relación a la seguridad de la información, la CSBP cuenta con una Encargada Nacional de Software Médico y Jefe Nacional en Telemática; con servidores redundantes (espejos); realizan copias de seguridad (*back up*); las agencias regionales envían diariamente el respaldo a la Oficina Nacional que centraliza toda la información; tienen una intranet; el médico, enfermera y personal administrativo cuentan con acceso a Internet (a excepción de redes sociales como Facebook, Twitter, otros); utilizan software propietario, pagan la licencia del software y antivirus; no llevan a cabo auditoría informática; y se encuentra en trámite la aprobación del Plan de Seguridad. Respecto a imagenología, la CSBP aún no cuenta con el sistema RIS-PAC pero se está proyectando la adquisición para el 2016. En relación a capacitación en TIC, cuentan con el curso teórico práctico de dactilografía médica, impartido a todos los médicos de Administraciones y Agencias Regionales con prácticas en *Typing Master* y las actualizaciones de los nuevos módulos del SAMI.

— La *Corporación del Seguro Social Militar (COSSMIL)* ha tenido malas experiencias en la implementación de sistemas de información en salud, es así que en el año 2004 una empresa boliviana desarrolló el Sistema de Gestión Hospitalaria (SIGEH), incluía software, equipamiento, cableado estructurado; el sistema contaba con veintiún (21) módulos, pero tuvo problemas por lo que el personal de la Dirección de Informática desarrolló el nuevo diseño del proyecto.

— Desde la gestión 2014 se ha desarrollado el *Sistema de Información Integrado de Control y Seguimiento Hospitalario (SISHAP)*, a la fecha cuenta con doce (12) módulos, entre ellos se encuentra el Módulo de Consulta Externa que permite al médico el acceso a la historia clínica electrónica; el médico accede a su perfil a través de un usuario y contraseña, una opción le permite reservar algunas enfermedades como el VIH-SIDA, por seguridad el médico no puede modificar la información de la historia clínica electrónica una vez que ha concluido el horario de la consulta externa; si necesita incluir alguna modificación, deberá hacerlo en el campo observaciones. El SISHAP se ha implementado también en las ciudades de Sucre y Puerto Suarez.

— En relación a la seguridad de la información, cuentan con un Director de Informática, se presenta una debilidad en los establecimientos de salud regionales en el cargo se encuentran Suboficiales que no son profesionales en informática, también existe mucha movilidad del personal; cuentan con servidores redundantes (espejos); realizan copias de seguridad *(back up)* de forma semanal; utilizan software propietario, pagan las licencias del software y antivirus; el desarrollo de los módulos del SISHAP se realiza bajo la modalidad de consultoría por producto; la capacitación de los módulos del SISHAP la realiza el Departamento de Informática de forma general y específica a los médicos.

— El trabajo de la Unidad de Archivo Clínico de COSSMIL ha sido reconocido por el Instituto Nacional de Seguros (INASES) y Servicio Departamental de Salud (SEDES) solicitando que realice capacitación a otros establecimientos de salud del subsector de seguridad social y subsector público. La Unidad de

Archivo Clínica cumple a estrictamente la Norma Técnica para el manejo del Expediente Clínico, también ha establecido sus propios protocolos para resguardar el acceso, integridad, confidencialidad, privacidad, custodia y seguridad de la historia clínica, gracias a estos mecanismos de control la Unidad de Archivo Clínico sabe exactamente dónde y con quién se encuentra la historia clínica del paciente.

— Como resultado de las entrevistas se percibe poca coordinación entre la Dirección de Informática, Unidad de Archivo Clínico, Auditoría Médica y otras unidades de COSSMIL para el desarrollo de los módulos del SISHAP, particularmente en lo relacionado a la Historia Clínica Electrónica. La Unidad de Archivo Clínico y Auditoría Médica consideran que por el momento el SISHAP no brinda la confidencialidad, privacidad y seguridad de la historia clínica en papel, esperan que haya un cambio en la Norma Técnica para el manejo del Expediente Clínico que reconozca el valor probatorio de la historia clínica electrónica y la firma electrónica.

— El *Seguro Social Universitario (SSU)* es una institución de servicio y derecho público, con personería jurídica, patrimonio propio, autonomía de gestión técnica, financiera y administrativa, que otorga prestaciones de salud a todos los trabajadores docentes y administrativos de la universidad boliviana. Todas las universidades estatales cuentan con el Seguro Social Universitario, a excepción del Departamento de Pando. La cita previa (ficha) para la consulta externa se solicita en forma presencial o por teléfono.

— La *Unidad de Bioestadística del SSU* esta encarga del procesamiento de los datos bioestadísticos que se encuentran en el Expediente Clínico, permite al SSU determinar cuáles son las enfermedades atendidas en el seguro, además de evaluar cuál es problema que genera este tipo de enfermedades. Para el registro de las enfermedades utiliza la Codificación Internacional de Enfermedades - CIE 10 que ha sido creada por la Organización Mundial de la Salud para uniformar y unificar los diagnósticos de las enfermedades de todo el mundo.

— La *Unidad de Admisión, Archivo y Fichaje del SSU* mantiene un registro detallado de la entrega a las enfermeras y devolu-

ción los expedientes clínicos. El expediente clínico está estructurado en consulta externa, laboratorios y exámenes complementarios y hospitalización. El médico de Consulta Externa del SSU de La Paz cuenta con el sistema Gema 1 y Gema 2 que contiene la historia clínica electrónica del paciente. El acceso al expediente clínico por parte del paciente se realiza mediante nota formal dirigida al Gerente de Salud del SSU, requerimiento fiscal u orden judicial. El préstamo de los expedientes clínicos a los estudiantes del último año de medicina que realizan internado rotatorio, médicos residentes, trabajadoras sociales, auditoría médica se realiza con el correspondiente registro. Las medidas de seguridad de la Unidad se resumen en puerta con llave y videovigilancia del SSU las 24 horas del día.

— El *personal de enfermería del SSU* es el encargado de abrir el expediente clínico del paciente, para lo cual solicita las tapas a la Unidad de Archivo, Admisión y Fichaje, también es responsable de realizar la verificación del llenado del expediente clínico, que tenga los datos generales del paciente, que no falte ningún campo, que haya sido llenado correctamente por el médico residente, que tenga la firma y pie de firma del médico tratante. Las enfermeras designadas a hospitalización (piso) revisan en detalle el expediente clínico para saber qué enfermedad tiene el paciente, cuales son las indicaciones que dio el médico, que medicamentos debe aplicar.

— El *Hospital Arco Iris (HAI)* es un hospital de segundo nivel que pertenece al sector privado sin fines de lucro, tiene una antigüedad de catorce (14) años, es un hospital de enseñanza, ha implementado hace dos (2) años el sistema *openHAI* que contiene a la historia clínica electrónica (HCE) de hospitalización, terapia intensiva (UTI), emergencias y consulta externa (desde septiembre de 2015[103]); este sistema es un desarrollo propio del

---

[103] La Fundación Arco Iris amplió sus servicios en salud e inauguró ayer el Centro Médico Arco Iris–Obrajes, que atenderá especialmente a la gente de la zona Sur las 24 horas, en al menos 15 especialidades. Este centro ambulatorio cuenta con todas sus consultas externas en al menos 15 especialidades: terapias intensivas adultas, pediátricas y neonatales, cirugía, gastroenterología, radiología, control de enfermedades no transmisibles (ENT), tomogra-

HAI que contó con la colaboración de un consultor italiano. El *openHAI* está compuesto de formularios que están acorde con la Norma Técnica para el manejo del Expediente Clínico. Para la creación de un formulario se requiere el consenso del Jefe de Servicio, médicos especialistas, enfermeras, el personal informático toma nota de los requerimientos y elabora el proyecto de formulario, con la validación de los futuros usuarios se procede a la implementación del mismo.

— Entre las *ventajas* que ofrece el *openHAI* está el autograbado cuando el médico va llenando la HCE; el acceso a la HCE desde cualquier dispositivo que tenga acceso a Internet (smartphone, tableta, computadora portátil o *smartTV*); cuenta con un Sistema de Almacenamiento de Imágenes Radiológicas (RIS) y el PACS, sistemas donde se almacenan las resonancias, tomografías, rayos X y cualquier otra imagen radiológica; facilidades para la impresión de la HCE porque cuenta con un servidor de impresoras.

— Entre las *desventajas* se podría considerar el respaldar la información de la HCE que son datos sensibles en servidores externos al Data Center del HAI, como el servicio que ofrece la nube (*cloud computing*), más aun si es un servicio gratuito se desconoce el paradero del alojamiento de los datos de la HCE; el acceso desde cualquier dispositivo que tenga acceso a Internet puede ir en contra de la confidencialidad de los datos del paciente contenidos en su HCE que puede ser vista por terceras personas que no sean el médico tratante o personal sanitario del HAI. Finalmente, la impresión de la historia clínica electrónica en la cual el médico debe colocar su nombre, firma y sello, porque todavía no se ha implementado la firma digital en el *openHAI*.

---

fía, mamografía, neumología, dermatología y estética general, entre otras. El centro cuenta con dos quirófanos ambulatorios, uno para cirugía mayor y otra para cirugía menor ambulatoria y con la sala de recuperación. Página Siete (2015), *«Arco Iris inaugura su centro de salud en la zona Sur»* periódico de circulación nacional [en línea]: http://www.paginasiete.bo/sociedad/2015/9/29/arco-iris-inaugura-centro-salud-zona-71696.html [Consulta: 30/09/2015].

9.2 CON RELACIÓN A LA HIPÓTESIS

Hipótesis: *La actual regulación en materia de protección de datos y seguridad de la información en Bolivia respecto del manejo de la historia clínica y la historia clínica electrónica es muy limitada, lo cual vulnera la protección en el tratamiento de los datos sanitarios afectando al derecho fundamental a la intimidad del paciente.*

— En materia de normativa sobre protección de datos personales, Bolivia cuenta con lo establecido en los artículos 130 y 131 Acción de Protección de Privacidad (ex Recurso de Hábeas Data) de la Constitución Política del Estado y el Capítulo Tercero Acción de Protección de Privacidad del Título II Acciones de Defensa del nuevo Código Procesal Constitucional. En el ámbito sanitario con la Ley 3131 del Ejercicio Profesional Médico, el Reglamento de la Ley del Ejercicio Profesional Médico (Decreto Supremo 28562) y la Norma Técnica para el manejo del Expediente Clínico (Resolución Ministerial 0090/2008).

— La Red Iberoamericana de Protección de Datos (RIPD) está conformada por veinticuatro (24) países; Bolivia, a través de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), forma parte de la RIPD desde 2005. Bolivia, a la fecha, no cuenta con una ley específica de protección de datos personales como los países que forman parte de la RIPD: España[104], Portugal[105], Andorra[106], Chile[107], Argentina[108], Uruguay[109], México[110],

---

104 Ley 15/1999 de Protección de Datos de Carácter Personal.

105 Ley 67/98 de Protección de Datos Personales de 26 de octubre.

106 Ley 15/2003 Qualificada de Protecció de dades personals de 18 de diciembre de 2013.

107 Ley 19628 Protección a la Vida Privada de 28 de agosto de 1999.

108 Ley 25326 de Protección de los Datos Personales de 2 de noviembre de 2000.

109 Ley 1833 Protección de Datos Personales y Acción de Hábeas Data de 11 de noviembre de 2008.

110 Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental de 11 de junio de 2002 y Ley Federal de Protección de Datos Personales en posesión de los Particulares de 5 de julio de 2010.

Perú[111], Costa Rica[112], Nicaragua[113], Colombia[114] y República Dominicana[115].

— La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) bajo tuición de la Vicepresidencia del Estado Plurinacional de Bolivia en la gestión 2009 promovió la elaboración de un «*Anteproyecto de Ley de Privacidad y Protección de Datos Personales*» para lo cual suscribió un Acuerdo de Intenciones con la Agencia Española de Protección de Datos. En la gestión 2009 se llevó a cabo la capacitación de dos (2) funcionarios de la ADSIB en la Agencia Española de Protección de Datos (Madrid - España), quiénes posteriormente elaboraron el primer Anteproyecto de Ley de Privacidad y Protección de Datos Personales. En su momento, la ADSIB buscó el apoyo del Ministerio de Transparencia Institucional y Lucha contra la Corrupción para que ambas entidades promuevan la socialización del Anteproyecto en la Asamblea Legislativa Plurinacional, pero la respuesta ha sido negativa por parte del Ministerio. En la gestión 2010, el Anteproyecto no llega a presentarse oficialmente en la Asamblea Legislativa. La ADSIB en los últimos años no participa en las reuniones y encuentros convocados por la Red Iberoamericana de Protección de Datos.

— El actual Gobierno es pro derecho de acceso a la información para evitar la corrupción y el enriquecimiento ilegítimo, para lo cual ha promovido la aprobación de la Ley de Lucha contra la Corrupción, enriquecimiento ilegítimo e investigación de fortunas «Marcelo Quiroga Santa Cruz» de fecha 31 de marzo de 2010, la cual levanta el secreto bancario a los funcionarios públicos (mientras duren en sus funciones). La Ley se utiliza con fines de persecución política a exautoridades y autoridades de los partidos políticos de oposición. No forma parte de la agen-

---

111 Ley 29733 de Protección de Datos Personales de 3 de julio de 2011.

112 Ley 8968 Protección de la Persona frente al tratamiento de sus datos personales de 7 de julio de 2011.

113 Ley 787 de Protección de Datos Personales de 29 de marzo de 2012.

114 Ley Estatutaria 1581 de 17 de octubre de 2012 por la cual se dictan disposiciones generales para la protección de datos personales.

115 Ley 172-13 Orgánica de Protección de Datos de Carácter Personal de la República de Dominicana de 26 de noviembre de 2013.

da del actual Gobierno velar por el «derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación», tanto es así que ha sido un escándalo público la actuación del ex Ministro de Salud, Juan Carlos Calvimontes, que en diciembre de 2014 convoca a conferencia de prensa para hacer público que el Magistrado del Tribunal Constitucional Plurinacional Gualberto Cusi «padece de una enfermedad terminal y tuberculosis (VIH-SIDA)».

— Pese a que en Bolivia existe una normativa que regula el secreto médico y la confidencialidad de los datos de salud, no es suficiente para precautelar el derecho fundamental que tienen las bolivianas y bolivianos a la intimidad y privacidad de los datos de salud considerados como «información sensible» por la jurisprudencia del Tribunal Constitucional (Sentencia Constitucional 0965/2004 de fecha 23 de junio de 2004). Por lo que se considera necesario que el Estado Plurinacional de Bolivia apruebe una Ley específica de Protección de Datos Personales que reconozca al titular del dato (persona natural o colectiva) sus derechos, determine las funciones del Responsable o Encargado del tratamiento de los datos personales, autorice la creación de una Autoridad de Control independiente en la cual se haga el registro de los archivos y bancos de datos públicos y privados, establezca las medidas técnicas y organizativas de seguridad de la información (nivel básico, medio y alto), asimismo, que ésta Autoridad tenga facultades de inspección y sanción.

— Las entrevistas realizadas a profesionales sanitarios (médicos, enfermeras, personal administrativo) de los establecimientos de salud del Sistema Nacional de Salud de la ciudad de La Paz alertan la falta de conocimiento de la normativa sobre la Acción de Protección de Privacidad, Ley del Ejercicio Profesional Médico, Norma Técnica para el manejo del Expediente Clínico, Consentimiento Informado, entre otras.

— La legislación de protección de datos es poco conocida por los profesionales, personal auxiliar y administrativo del ámbito sanitario boliviano; se debe fortalecer más la formación en esta materia. Se debe incrementar la formación en el Sistema Nacional de Salud boliviano, hacer una campaña de concienciación sobre protección de datos personales en los equipos y directi-

vos de los centros, responsables administrativos relacionados con el manejo y difusión de datos, responsables de admisión y archivos, responsables y personal de informática y responsables de las unidades de atención al paciente.

— El derecho de acceso a la historia clínica por parte del paciente se realiza mediante carta formal dirigida al Gerente de Salud del establecimiento de salud (laboratorios, préstamo de radiografías o tomografías, epicrisis, otros), si el paciente requiere el expediente clínico completo debe hacer su solicitud por requerimiento fiscal u orden judicial. El establecimiento de salud entregará al paciente, familiar o representante legal una fotocopia legalizada debidamente foliada. En el ámbito sanitario el expediente clínico se considera un documento legal.

— La Norma Técnica para el manejo del Expediente Clínico establece que el manejo del expediente clínico debe ser cuidadoso, con anotaciones en letra completamente legible y de fácil comprensión. Son inaceptables dado el carácter de documento médico-legal la letra ilegible, tachaduras, enmiendas sobrepuestas o aledañas a la propia escritura, si es necesario hacer alguna modificación o aclaración debe ser hecha en nota o indicación aparte debidamente refrendada con el nombre, firma, fecha y hora de quien la realice.

— Esta medida de seguridad en la historia clínica electrónica se debe registrar en otro campo que se denomina «observaciones», «anotaciones», «hoja o nota de evolución», otros. En el caso de la Caja de Salud de la Banca Privada (CSBP) la modificación de la historia clínica electrónica corresponde con autorización y en presencia del Supervisor de Software Médico; en la historia clínica electrónica del Hospital Arco Iris (HAI) el plazo para la modificación es de 24 horas; en la Corporación del Seguro Social Militar (COSSMIL) la modificación a la historia clínica electrónica se la puede realizar durante el horario de la consulta externa, caso contrario si la modificación se la quiere hacer al día siguiente deberá registrarla en el campo de «observaciones». Por lo antes expuesto, se considera la historia clínica electrónica más segura y confidencial que la historia clínica en papel, hay mayores medidas de seguridad en los ficheros electrónicos si establecen perfiles de usuarios para las vistas (médico, enfermera,

personal administrativo), claves de acceso (firma electrónica) y se conoce el rastro de todos los accesos *(logs)*.

— La Unidad de Archivo y Estadísticas realiza el control, archivo, conservación y custodia de la historia clínica conforme establece la Norma Técnica para el manejo del Expediente Clínico. Las entrevistas han permitido conocer que cuando existe requerimiento del expediente clínico por causas legales, auditoria médica externa o peritaje hay colaboración y solidaridad entre médicos, enfermeras y personal administrativo para completar la información que debe contener la historia clínica (métodos auxiliares de diagnóstico, notas de evolución, tratamientos, consentimiento informado, documentos administrativos, refrendados todos con nombre, firma, y sello o identificación escrita de las personas responsables), lo cual demuestra la poca integridad y seguridad que ofrece las historia clínica en papel.

— La Norma Técnica para el manejo del Expediente Clínico que es de observación y cumplimiento obligatorio en todo el Sistema Nacional de Salud de Bolivia no considera en forma expresa a la historia clínica electrónica. Sin embargo, menciona en algunos artículos los términos: «tecnológicos», «mediante cualquier recurso técnico», «copia magnética», «fotocopia».

— Por otra parte, con la implementación de la historia clínica electrónica la Unidad de Archivo y Estadísticas del establecimiento de salud será la encargada de realizar el control, archivo, conservación y custodia de la historia clínica en papel; en cambio la Dirección de Informática, Unidad de Sistemas, Unidad de Telemática será la encargada del control, archivo, conservación y custodia de la historia clínica electrónica. Por la inclusión de las TIC en el ámbito sanitario se considera pertinente la actualización de la Norma Técnica para el manejo del Expediente Clínico.

— Es más eficiente implantar un sistema de historia clínica de manera gradual, evitando una implantación a gran escala al principio para evitar que la implantación falle provocando problemas complejos y se propague un efecto en cadena y provoque una resistencia del personal a la nueva iniciativa. Por eso la gestión de la implantación de infraestructuras de tecnologías de la información y comunicaciones se debe la llevar con una

visión estratégica totalmente distinta a la tradicional, esto evitará que proyectos de transformación y gran envergadura fracasen o se tengan resultados que no correspondan a la magnitud del esfuerzo desarrollado.

— Se destaca el Software Médico y Sistema Administrativo Médico (SAMI) de la Caja de Salud de la Banca Privada (CSBP) implementado hace casi 10 años. Se observa confidencialidad y reserva en el tratamiento de los datos de la historia clínica electrónica del paciente; el desarrollo de los módulos del SAMI se realiza en etapas, antes de su implementación tiene bastante socialización y consenso entre el personal sanitario; tiene adecuadas medidas de seguridad de la información (software seguro, perfiles de acceso, servidores redundantes, copias de seguridad, cortafuegos, otros); una inversión anual en hardware y software; capacitación de uso de TIC al personal sanitario a través de una plataforma de e-learning entre otras ventajas. El SAMI ha ido mejorando, complementando y actualizando de acuerdo a las necesidades institucionales de la CSBP. El SAMI se encuentra implementado casi en todos los departamentos de Bolivia.

— La Corporación del Seguro Social Militar (COSSMIL) ha desarrollado dentro del Sistema de Información Integrado de Control y Seguimiento Hospitalario (SISHAP) el módulo de Historia Clínica Electrónica (tiene 1 año de implementación). Las entrevistas realizadas han permitido conocer que no existe una coordinación interna entre el Departamento de Informática, la Unidad de Archivo Clínico, Auditoria Médica y otras unidades implicadas en el desarrollo de los módulos del SISHAP, lo que ha ocasionado malestar interno y falta de credibilidad en las medidas de seguridad de la información en el llenado de la historia clínica electrónica donde se puede observar registros como «ver sistema» o «tratamiento igual que el anterior», confirmando la posición de la Unidad de Archivo Clínico y Auditoria Médica que la historia clínica en papel es más completa, segura y confidencial. Por otra parte, el médico (principal usuario del módulo de la historia clínica electrónica) no brinda tiempo ni suficiente atención al personal del Departamento de Informática para la capacitación. Decisiones del alto mando de COSSMIL consideran que con la implementación de la historia

clínica electrónica la historia clínica en papel debe desaparecer, ser reciclada o destruida, pero sin las adecuadas medidas de seguridad.

— Un común denominador entre los funcionarios entrevistados en la Caja de Salud de la Banca Privada, Corporación del Seguro Social Militar, Seguro Social Universitario y Hospital Arco Iris es el desconocimiento del valor jurídico probatorio del documento digital (que en ámbito sanitario se traduce en la historia clínica electrónica) y la firma digital, ambos regulados en la Ley 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación y su Decreto Reglamentario. Todos los funcionarios esperan que el valor jurídico probatorio de la historia clínica electrónica y la firma digital esté establecido en la Norma Técnica para el Manejo del Expediente Clínico. Por otra parte, hay desconocimiento en los funcionarios en qué consiste y como se aplica la firma digital a la historia clínica electrónica, considerando en algún caso que el establecimiento de salud debe constituirse en Entidad Certificadora autorizada y cumplir con los requisitos técnicos, legales y económicos establecidos por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

— La Ley 164 General de Telecomunicaciones, Tecnologías de Información establece como prioridad nacional la promoción del uso de las tecnologías de información y comunicación para procurar el vivir bien de todas las bolivianas y bolivianos. Señala que las entidades públicas deben adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las tecnologías de información y comunicación en el desarrollo de sus funciones. Asimismo, el Estado debe promover el desarrollo de contenidos, aplicaciones y servicios de las tecnologías de información y comunicación en la salud, como mecanismo para desarrollar el sistema de alerta temprana, bases de administración de recursos en salud y plataformas de acceso a la información y consultas del sector.

— Bolivia ha realizado una inversión económica de más de 300 millones de dólares en la adquisición del satélite «Tupac Katari» para poder brindar mayor acceso y conectividad al área rural. El proyecto nacional de «Telesalud para Bolivia» con-

templa la utilización del nuevo satélite «Tupac Katari»; tiene como objetivo demostrar que es viable desarrollar e implementar herramientas de telemedicina en instituciones gubernamentales y municipales de salud. En el Estado Plurinacional de Bolivia no existe, por el momento, una regulación del uso de las herramientas de telemedicina. Sin embargo, el Proyecto utiliza el documento *«Declaración de la Asociación Médica Mundial sobre las responsabilidades y normas éticas en la utilización de la telemedicina»* de la OMS para alcanzar acuerdos con las instituciones participantes.

— La Ley 164 también establece la conformación del Comité Plurinacional de Tecnologías de Información y Comunicación (COPLUTIC), con la finalidad de proponer políticas y planes nacionales de desarrollo del sector de tecnologías de información y comunicación, coordinar los proyectos y las líneas de acción entre todos los actores involucrados, definir los mecanismos de ejecución y seguimiento a los resultados. Pese a lo expuesto, el Sistema Nacional de Salud (SNS) boliviano no cuenta con una política pública que establezca las directrices para la utilización de las tecnologías de la información y comunicación (TIC) en el ámbito de la salud.

9.3 FUTURAS LÍNEAS DE INVESTIGACIÓN

Historia Clínica Única: El Sistema Nacional de Salud de Bolivia requiere contar con una Historia Clínica Única que contenga la información del paciente registrado con un solo código a nivel nacional que puede ser la Cédula de Identidad, proponer un modelo que se pueda ajustar a la realidad boliviana.

Historia Clínica Personal: Los pacientes pueden aprovechar el acceso a la información para mejorar su salud y la gestión de sus enfermedades. Los sistemas de historias clínicas personales son más que simples repositorios estáticos para los datos del paciente; se combinan los datos, conocimientos y herramientas de software que ayudan a los pacientes a convertirse en participantes activos en su propio cuidado. Múltiples actores como pacientes, proveedores de servicios de salud, empleadores, contribuyentes, gobiernos e instituciones de

investigación, juegan un papel clave en el desarrollo de la tecnología de la Historia Clínica Personal.

Cloud computing: Los servicios de cómputo en la nube *(cloud computing)* presentan retos a los sistemas jurídicos nacionales, internacionales y por ello se requiere partir de un marco claro y transparente en el ámbito contractual, donde empresas y gobierno se comprometan a lograr los mejores resultados y cumplir con los derechos que están en juego respecto de la información del mismo Estado y de los habitantes y/o ciudadanos y en particular el tratamiento de los datos personales en el ámbito sanitario.

Big Data: Los principios básicos de la protección de datos personales son plenamente aplicables al Internet de las Cosas (iot) y al fenómeno del big data. A pesar de que los diferentes objetos que conforman la internet de las cosas recogen piezas aisladas de información, los datos recogidos de diferentes fuentes y analizados de otra forma o en conjunción con otros pueden revelar aspectos específicos de hábitos, comportamientos y preferencias, configurando auténticos patrones de la vida de las personas. Es razonable pensar que el sector sanitario integrará toda esta información y la utilizará en beneficio de las personas.

9.4 TRABAJOS DERIVADOS

2015: *«La seguridad de la información clave en la protección de datos sanitarios»,* Fuentes Revista de la Biblioteca y Archivo Histórico de la Asamblea Legislativa Plurinacional Año 14, Volumen 9, Número 38, junio 2015, ISSN 2225-3769 – D.L. 4-3-96-02, La Paz – Bolivia.

2013: *«Políticas en tecnologías de la información y comunicación en el nuevo contexto social y educativo en Bolivia»,* Observatorio Iberoamericano del Desarrollo Local y la Economía Social, Vol. 7, 14 (junio 2013), ISSN: 1988-2483, Universidad de Málaga – España: http://www.eumed.net/rev/oidles/14/educacion-bolivia.pdf

2013: *«Transparencia y acceso a la información en Bolivia»*. Fuentes Revista de la Biblioteca y Archivo de la Asamblea Legislativa Plurinacional, Año 12, Volumen 7, Número 24, Febrero 2013. ISSN 2225-3769 – D.L. 4-3-96-02, La Paz – Bolivia.

2010: *«Normativa en tecnologías de la información y la comunicación en la sociedad de la información de Bolivia»*, Revista Científica Digital Diálogos Transdisciplinarios en la Sociedad de la Información, Junio 2010, ISSN 2220-7120, La Paz – Bolivia.

2005: *«Construyendo el e-government en Bolivia»*, IADIS Conferencia Ibero – Americana CIAWI 2005, Octubre 18 – 19 de 2005, Lisboa – Portugal. ISBN 972-8924-03-08.

2005: *«Data security involvement: in search of EHR compliance»*, IADIS International Conference e-Society 2005, Junio 27 – 30 de 2005, Qawra – Malta. ISBN 972-8939-03-5.

2005: *«El outsourcing clave de éxito en la empresa actual»*, Libro de comunicaciones de la I Jornada Académica de Postgrado de Investigación en Ingeniería Informática de la UPSA, Salamanca, 2004. ISBN: 84-688-6550-8.

BIBLIOGRAFÍA

ABAD, I., y CARNICERO, J. (2012). *«Intercambio internacional de información clínica»* en «Manual de Salud electrónica para directivos de servicios y sistemas de salud» [en línea]: http://repositorio.cepal.org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 04/05/2015].

ABELLÁN S., J. C.; BARRACA M., J., *et al.* (2007). *«La praxis del consentimiento informado en la relación sanitaria»*. Editor Difusión Jurídica y Temas de Actualidad, S. A. Madrid.

ACEITUNO C., V. (2004). *«Seguridad de la Información»*. Creaciones Copyright, S. L. España.

AGENCIA DE CALIDAD SANITARIA DE ANDALUCÍA (2015). *«Certificación de webs y blogs sanitarios»* [en línea]: http://www.juntadeandalucia.es/agenciadecalidadsanitaria/certificacion-acsa/certificacion-de-webs-y-blogs-sanitarios/ [Consulta: 25/06/2015].

AGENCIA DE LOS ESTADOS UNIDOS PARA EL DESARROLLO INTERNACIONAL (2015). *«Programa de Cooperación USAID en Bolivia»* [en línea]: http://spanish.bolivia.usembassy.gov/usaid.html [Consulta: 07/05/2015].

AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID (2004). *«Guía de Protección de Datos Personales para Servicios Sanitarios Públicos»*. Civitas Ediciones, S. L. Madrid.

— (2004). *«Memoria 2004»*. Edita Agencia de Protección de Datos de la Comunidad de Madrid. España.

— (2008). *«Protección de datos personales para Servicios Sanitarios Públicos»*. Edita Agencia de Protección de Datos de la Comunidad de Madrid. Madrid.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2000). *«Manual de Protección de Datos Personales»*. Edita Agencia Española de Protección de Datos. Madrid.

— (2010). *«Informe de cumplimiento de la LOPD en Hospitales»* [en línea]: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/octubre/Informe_cumplimiento_LOPD.pdf [Consulta: 11/04/2015].

— (2013). *«Guía para clientes que contraten servicios de Cloud Computing»* [en línea]: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf [Consulta: 15/06/2015].

— (2014). *«Memoria 2013»* [en línea]: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2013/Memoria_AEPD_2013.pdf [Consulta: 20/07/2014].

— (2015). *«Transferencia internacionales de datos»* [en línea]: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php#paises [Consulta: 18/06/2015].

— (2015). *«El TJUE declara inválida la Decisión de la Comisión que declara el nivel adecuado de protección de Puerto Seguro»* [en línea]: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_06-ides-idphp.php [Consulta: 18/10/2015].

AGUILERA LÓPEZ, P. (2010). *«Seguridad informática»*. Editorial Editex. Madrid.

ALONSO, J. M.; GARCÍA, J. L.; SOTO, A., *et al.* (2009). *«La protección de datos personales: Soluciones en entornos Microsoft Versión 2.0»*. Microsoft Ibérica S.R.L. Madrid.

ÁLVAREZ-CIENFUEGOS S, J. M. (2000). *«La Historia Clínica: custodia y propiedad»*, en «I Jornadas de Protección de Datos Sanitarios en la Comunidad de Madrid». Editorial MAPFRE, S. A. Madrid.

— (2001). *«La Aplicación de la Firma Electrónica y Protección de Datos relativos a la Salud»*. Revista Actualidad Informática Aranzadi, Número 39, abril de 2001.

AMAYA A, J. (2010). *«Sistemas de información gerenciales: hardware, software, redes, internet, diseño»*. Ecoe Ediciones. Bogotá.

APARICIO S., J. (2000). *«Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal»*. Editorial Aranzadi, S. A. Navarra.

APONTE G. (2014). *«Seguro Universal de Salud»* en «Bolivia encrucijadas en el siglo XXI» Editora Presencial SRL, La Paz.

ARCE J., J. A. (2003). *«Informática y Derecho»*. Ediciones Instituto Boliviano de Investigaciones Jurídicas. La Paz.

ARMIJO S., F., *et al.* (1993). *«Experiencias del proceso de implementación y resultados de los dos primeros años de funcionamiento (1991 y 1992), del Subsistema Nacional de Información en Salud: SNIS»*. Sistema Nacional de Información en Salud, La Paz-Bolivia.

ASOCIACIÓN DE BANCOS PRIVADOS DE BOLIVIA (2015). *«Misión»* [en línea]: http://www.asoban.bo/certificados/manuales [Consulta: 30/09/2015].

ASOCIACIÓN IBIS-HIVOS (2008). *«Trabajo con personas viviendo con VIH/SIDA»* [en línea]: http://www.ibis-hivos.net/tsc1.asp?seccion=pvvs [Consulta: 07/10/2008].

ATELA B., A., y GARAY I., J. (2004). *«Ley 41/2002 de Derechos del Paciente. Avances, Deficiencias y Problemática»* en González S., P., Lizárraga B., E. *et al.* (2004). «Autonomía del Paciente, Información e Historia Clínica». Civitas Ediciones, S. L. Madrid.

AYALA S., M. A. (2013). *«Plan de Desarrollo de la propuesta para mejorar el análisis, seguimiento y reportes de indicadores estratégicos de salud de la política y en seguimiento a los ODMS 4 y 5»*, Consultoría para el Ministerio de

Salud y Deportes, Organización Panamericana de la Salud y Organización de la Salud, La Paz - Bolivia.

BANCO MUNDIAL (2012). *«Information and Communications for Development 2012: Maximizing Mobile»*, Washington, D.C. [en línea], http://publications.worldbank.org/index.php?main_page=product_info&products_id=24288 [Consulta: 17/06/2005].

BETELU C., K. (2014). *«La informática en los servicios de urgencias extrahospitalarias»* en en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud. Volumen II Aplicaciones de las TIC a la atención primaria de salud» Publicación de las Naciones Unidas [en línea]: http://www.seis.es/documentos/X%20Informe%20SEIS%20-%20COMPLETO.pdf [Consulta: 20/06/2015].

BLANCO, O., y ROJAS, D. (2012). *«Principios de seguridad de información en entornos de salud»* en «Manual de Salud electrónica para directivos de servicios y sistemas de salud» [en línea]: http://www.seis.es/documentos/informes/secciones/adjunto1/16_Principios_de_seguridad_de_la_informacion_en_entornos_de_salud.pdf [Consulta: 04/05/2015].

BLAS O., C. (2006). *«El equilibrio en la relación médico - paciente»*. Bosch Editor. Navarra.

BLUMENTHAL, D., y TAVENNER, M. (2010). *«The Meaningful Use Regulation for Electronic Health Records»*, N Engl J Med, vol. 363, N.º 6 citado por González B., F. y Luna, D. (2012): *«La historia electrónica»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud». Publicación de las naciones Unidas enero de 2012 [en línea]: http://repositorio.cepal.org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 22/03/2015].

BOLETÍN OFICIAL DEL ESTADO (2003). «*Ley 59/2003 de 19 de diciembre de Firma Electrónica»*.

BOLIVIA EMPRENDE (2014). *«SOBOCE premió a 61 ganadores de concurso Emprendeideas»* [en línea]: http://boliviaemprende.com/noticias/soboce-premio-61-ganadores-de-concurso [Consulta: 20/06/2015].

BOYLE, R. J., y PANKO, R. R. (2013). *«Access control»* Corporate Computer Security, Upper Saddle River. Nueva Jersey.

BUSTAMANTE D., J. (2013). *«Ética en la nube: Dilemas éticos y políticos en el modelo de Computación en Nube (Cloud Computing)»*. Universidad Complutense de Madrid [en línea]: https://www.academia.edu/4873076/%C3%89TICA_EN_LA_NUBE_DILEMAS_%C3%89TICOS_Y_POL%C3%8DTICOS_EN_EL_MODELO_DE_COMPUTACI%C3%93N_EN_NUBE_CLOUD_COMPUTING_2013_ETHICS_ON_THE_CLOUD_ETHICAL_AND_POLITICAL_DILEMMAS_IN_THE_MODEL_OF_CLOUD_COMPUTING [Consulta: 30/09/2015].

BUSTILLOS, M. (2015). *«Software de Atención Primaria en Salud (SOAPS)»* entrevista al Encargado del SOAPS del Sistema Nacional de Información en Salud (SNIS) en fecha 23/07/2015 en la ciudad de La Paz, Bolivia.

CAJA DE SALUD DE LA BANCA PRIVADA (2014). *«Acerca de la CSBP»* [en línea]: http://portal.csbp.com.bo/inicio/index.php/acerca-de-la-c-s-b-p/acerca-de-la-c-s-b-p [Consulta: 25/12/2014].

— (2015): *«Memoria Anual 2014»* [en línea]: http://portal.csbp.com.bo/inicio/attachments/article/1561/MEMORIA%20CSBP%202014.pdf [Consulta: 30/06/2014].

CALVO S., M. D. (2006). *«Protección de datos personales a través del secreto profesional en el ámbito de la Administración Sanitaria Local»* en Revista de Estudios de la Administración Local y Autonómica (enero-agosto 2006). Edita Instituto Nacional de Administración Pública, Madrid.

CAMPUZANO T., H. (2000). *«Vida Privada y Datos Personales»*. Editorial Tecnos, S. A. Madrid.

CAO, J. (2013). *«El control A.7.2 «Clasificación de la información» de la norma ISO 27001 y la norma ISO 30301 (1ra parte»)* [en línea]: http://www.iso30300.es/el-control-a-7-2-clasificacion-de-la-informacion-de-la-norma-iso-27001-y-la-norma-iso-30301-1a-parte/ [Consulta: 01/05/2015].

CARNICERO G., J. (2003). *«De la Historia Clínica a la Historia de Salud Electrónica (Resumen)»*.Sociedad Española de Informática de la Salud (SEIS) [fuera de línea]: http://www.seis.es/informes/2003/PDF/CAPITULO1.pdf [Consulta: 20/06/2005].

— (2004). «*La Historia Clínica Informatizada»*, en León S., P. (2004). «La Implantación de los Derechos del Paciente». Ediciones Universidad de Navarra, S. A. Pamplona.

CARNICERO G., J.; ROJAS DE LA ESCALERA, D. y BLANCO R., O. (2014). *«La gestión de la función TIC en los servicios de salud: algunos errores frecuentes de los equipos de dirección»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud. Volumen II Aplicaciones de las TIC a la atención primaria de salud» Publicación de las Naciones Unidas [en línea]: http://www.seis.es/documentos/X%20Informe%20SEIS%20-%20COMPLETO.pdf [Consulta: 20/03/2015].

CARNICERO, J.; AMÉZQUETA, C., y GRANADO, A. (2003). *«De la Historia Clínica a la Historia de Salud Electrónica (Conclusiones) V Informe»*. Sociedad Española de Informática de la Salud (SEIS) [en línea]: http://www.conganat.org/SEIS/informes/2003/PDF/CONCLUSIONES.pdf [Consulta: 20/03/2015].

CARNICERO, J.; RIESGO, I.; GARBAYO, J.A., y QUIRÓS J.M. (2002). *«Algunas directrices estratégicas para los sistemas de información de los servicios de salud»*. Revista Todo Hospital, Número 191, pp. 649-658.

CENTROS DEPARTAMENTALES DE VIGILANCIA, INFORMACIÓN Y REFERENCIA (2015). *«Qué es el CDVIR»*, La Paz - Bolivia.

CHAUDRY, B., y otros (2006). *«Systematic Review: Impact of Health Information Technology on Quality, Efficiency and Costs of Medical Care»*, Ann Intern Med. Vol. 144, N.º 10 citado por González B., F. y Luna, D. (2012): *«La historia electrónica»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud». Publicación de las naciones Unidas enero de 2012 [en línea]: http://repositorio.cepal.org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 22/03/2015].

CHEN, T. C., y otros (2011). *«Computer laboratory notification system via short message service to reduce health care delays in management of tuberculosis in Taiwan»* [en línea]: http://www.ncbi.nlm.nih.gov/pubmed/21496958 [Consulta: 22/06/2015].

CIMINO, J., y DEL FRIOL, G. (2007). *«Infobuttons and Point of Care Access to Knowledge»* en R.A. Greenes (Ed.), Clinical decisión support-the road abead. Amsterdam: Elsever Academic Press citado por González B., F. y Luna, D. (2012): *«La historia electrónica»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud». Publicación de las naciones Unidas enero de 2012 [en línea]: http://repositorio.cepal.org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 22/03/2015].

CORBELLA D., J. (2006). *«Manual de Derecho Sanitario»*. Atelier Libros Jurídicos. Barcelona.

CORPORACIÓN DEL SEGURO SOCIAL MILITAR (2008). *«Memoria Anual 2006»*. Edición Unidad de Imagen Corporativa COSSMIL, Impresión Artes Graficas Sagitario S.R.L., La Paz.

— (2014). *«Guía Institucional»* [en línea]: http://www.cossmil.mil.bo/junta-superior-de-decisiones.aspx [Consulta: 24/12/2014].

— (2014). *«Guía Institucional»* [en línea]: http://www.cossmil.mil.bo/home.aspx [Consulta: 24/12/2014].

CRIADO DEL RÍO, M. T. (1999). *«Aspectos Médico – Legales de la Historia Clínica»*. Editorial COLEX. Madrid.

CUENTAS, G. (2015). *«Salud y proceso de cambio»* en «El cambio a fondo» edición especial quinto aniversario del periódico de circulación nacional Página Siete 19 de abril de 2015.

CURIOSO V., W. (2014). *«Salud móvil en atención primaria»*en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud. Volumen II Aplicaciones de las TIC a la atención primaria de salud» Publicación de las Naciones Unidas [en línea]: http://www.seis.es/documentos/X%20Informe%20SEIS%20-%20COMPLETO.pdf [Consulta: 10/06/2015].

DAVARA R., M. (2005). *La seguridad en las transacciones electrónicas: La Firma Electrónica.* Editorial Vodafone Fundación España. Madrid

Decreto Ley 15629 *«Código de Salud de la República de Bolivia»* de fecha 18 de julio de 1078 [en línea]: http://inases.gob.bo/wp-content/marco_legal/codigo_salud.pdf [Consulta: 20/03/2015].

Decreto Supremo 18886 *«Reglamentos concernientes al Código de salud»* de fecha 15 de marzo de 1982.

DE LORENZO Y MONTERO, R. (2003). *«Derechos y Obligaciones de los Pacientes»*. Editorial COLEX. Madrid.

DEL PESO N., E. (2003). *«Servicios de la Sociedad de la Información. Comercio Electrónico y Protección de Datos»*. Ediciones Díaz de Santos, S. A. Madrid.

DEL PESO N., E.; RAMOS G., M. A., y DEL PESO R., M. (2004). *«El Documento de Seguridad. Análisis Técnico y Jurídico. Modelo»*. Ediciones Díaz de Santos, S. A. Madrid.

DE MIGUEL S., N. (2002). *«Secreto Médico, Confidencialidad e Información Sanitaria»*. Marcial Pons Ediciones Jurídicas y Sociales, S. A. Madrid.

— (2004). *«Tratamiento de Datos Personales en el Ámbito Sanitario: Intimidad «versus» Interés Público»*. Edita Tirant Lo Blanch. Valencia.

DE QUINTO Z., F. (2004). *»La firma electrónica. Marco legal y aplicaciones prácticas»*. Editor Difusión Jurídica y Temas de Actualidad, S. A., Barcelona.

DIARIO PÁGINA SIETE (2014). *«El ministro busca que enfermos de VIH-Sida sean estigmatizados»* [en línea]: http://www.paginasiete.bo/sociedad/2014/12/27/ministro-busca-enfermos-vih-sida-sean-estigmatizados-42383.html [Consulta: 19/01/2014].

EL PAÍS (2015). *«Claves de la nueva Ley de Propiedad intelectual»* [en línea]: http://cultura.elpais.com/cultura/2015/01/05/actualidad/1420459097_337231.html [Consulta: 15/09/2015].

ESQUIVEL, A., y UZQUIANO G. (2008). *«Programa desnutrición cero de Bolivia: objeto de estudio e intervención desde el modelo conceptual de salud internacional. Informe Final»* [en línea]: http://www.bvsde.ops-oms.org/texcom/nutricion/proyecto-final.pdf [Consulta: 08/06/2015].

FALAGÁN M., J. A., y NOGUEIRA F., J. (2003). *«La Información Clínica y de Salud»*. Sociedad Española de Informática de la Salud (SEIS)[en línea]:http://www.conganat.org/SEIS/informes/2003/PDF/CAPITULO3.pdfhttp://www.conganat.org/SEIS/informes/2003/PDF/CAPITULO3.pdf [Consulta: 20/03/2015].

FERNÁNDEZ A., M. (2004). *«Las TI y su aplicación en Ciencias de la Salud»*, en Revista de Ciencias Sociales Sociedad y Utopía. Edita Facultad de CC.PP. y Sociología León XIII y Fundación Pablo VI. Madrid.

FERNÁNDEZ-MEDINA P., E.; MOYA Q., R., y PIATTINI V., M. (2003). *Seguridad de las tecnologías de la información*. Ediciones AENOR. Madrid.

FUNDACIÓN ARCO IRIS (2015). *«Hospital Arco Iris»* [en línea]: http://www.arcoirisbolivia.org/mision.html [Consulta: 07/01/2015].

FURUKAWA, M. F. (2011). *«Electronic Medical Records and Efficiency and Productivity During Office Visits»*, Am J Manag Care, vol. 17 N.º 4 citado por González B., F. y Luna, D. (2012): *«La historia electrónica»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud». Publicación de las naciones Unidas enero de 2012 [en línea]: http://repositorio.cepal.

org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 22/03/2015].

GABARRÓN, E., y FERNÁNDEZ-LUQUE, L. (2012). *«eSalud y videos online para la promoción de la salud»* Gaceta Sanitaria, vol. 26, N.º 3 [en línea]: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0213-91112012000300001 [Consulta: 25/06/2015].

GACETA OFICIAL DEL ESTADO PLURINACIONAL DE BOLIVIA (2005). *«Decreto Supremo N.º 28168 de acceso a la información al Poder Ejecutivo de fecha 17 de mayo de 2005»*.

— (2005). *«Ley N.º 3131 del Ejercicio Profesional Médico de fecha 8 de agosto de 2005»*.

— (2007). *«Ley N.º 3729 Ley para la prevención del VIH-SIDA de fecha 8 de agosto de 2007»*.

— (2009). *«Constitución Política del Estado Plurinacional de Bolivia de fecha 7 de febrero de 2009»*.

— (2009). *«Decreto Supremo N.º 066 Bono Madre Niño - Niña «Juana Azurduy» de fecha 3 de abril de 2009»*.

— (2010). *«Decreto Supremo N.º 29894 Estructura organizativa del Poder Ejecutivo del Estado Plurinacional de fecha 7 de febrero de 2009»*.

— (2010). *«Decreto Supremo N.º 0451* reglamenta las disposiciones contenidas en la Ley 3729 de fecha 8 de agosto de 2007 de fecha 8 de agosto de 2007 para la prevención del VIH-SIDA reglamenta las disposiciones contenidas en la Ley 3729 de fecha 8 de agosto de 2007 de fecha 8 de agosto de 2007 para la prevención del VIH-SIDA *de fecha 7 de febrero de 2009»* de fecha 17 de marzo de 2010.

— (2010). *«Ley 031 de Autonomías y Descentralización «Andrés Ibáñez» de fecha 19 de julio de 2010»*.

— (2011). *«Ley 164 General de Telecomunicaciones, Tecnología de Información y Comunicación de fecha 8 de agosto de 2011»*.

— (2012). *«Código Procesal Constitucional de fecha 5 de julio de 2012»*.

— (2013). *«Decreto Supremo 1793 Reglamento a la Ley 164 para el desarrollo de Tecnologías de Información y Comunicación de fecha 13 de noviembre de 2013»*.

— (2013). *«Ley 475 de Prestaciones de Servicios de Salud Integral del Estado Plurinacional de Bolivia de fecha 30 de diciembre de 2013»*.

GAIERO, B.J., y SOBA, I.M. (2010). *«La regulación procesal del hábeas data»*. Editorial B de F Ltda, Montevideo.

GARBAYO S., J. A.; Sans U., J.; CARNICERO G., J., Y SÁNCHEZ G., C. (2003). *«La Seguridad, Confidencialidad y Disponibilidad de la Información Clínica»*. DOCPLAYER [en línea]: http://docplayer.es/6816823-La-seguridad-confidencialidad-y-disponibilidad-de-la-informacion-clinica.html [Consulta: 15/06/2015].

GARCÍA, A. (2012). *«El sistema de información del hospital»* en Manual de Salud electrónica para directivos de servicios y sistemas de salud [en línea]: http://www.seis.es/documentos/informes/secciones/adjunto1/01_El_sistema_de_informacion_del_hospital.pdf [Consulta: 04/05/2015].

GARCÍA-BERRIO H., T. (2003). *«Informática y libertades. La protección de datos personales y su regulación en Francia y España»*. Servicio de Publicaciones de la Universidad de Murcia, Murcia.

GARCÍA B., J. (2003). *«Medicina Legal: responsabilidad por las actuaciones sanitarias»*. Editorial Formación Alcalá. Jaén.

GARCÍA M., F. J. (2004). *«Comercio y firma electrónicos (análisis jurídico de los servicios de la sociedad de la información)»*. Editorial Lex Nova, Segunda Edición, Valladolid.

GARRIGA D., A. (2004). *«Tratamiento de Datos Personales y Derechos Fundamentales»*. Editorial Dykinson, S. L. Madrid.

GINER DE LA FUENTE, F., y GIL E., M. (2004). *Los Sistemas de información en la sociedad del conocimiento*. Editorial ESIC. Madrid.

GOBIERNO AUTÓNOMO DEPARTAMENTAL DE LA CIUDAD DE LA PAZ (2010). *«Programa Departamental de ITS/VIH/SIDA»*. Servicio Departamental de Salud [en línea]: http://www.sedeslapaz.gob.bo/index.php?option=com_content&view=article&id=114:psida&catid=41:peer&Itemid=112 [Consulta: 15/08/2015].

GOBIERNO AUTÓNOMO MUNICIPAL DE SANTA CRUZ (2015). «Defensoría de la Niñez y Adolescencia» [en línea]: http://www.dnamunicipal.cotas.net/dna.htm [Consulta: 15/08/2015].

GONZÁLEZ B., F., y LUNA, D. (2012). *«La historia electrónica»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud». Publicación de las naciones Unidas enero de 2012 [en línea]: http://repositorio.cepal.org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 22/03/2015].

GONZÁLEZ DEL ALBA B., A (2015). *«Diseño de una arquitectura informática para la implantación de la Historia Clínica Digital: Integración de los Agentes Inteligentes, Sistemas Multiagente y Servicios Web»* Tesis Doctoral de la Universidad Pontificia de Salamanca, Madrid.

GONZÁLEZ M., J. (2005). *«Historia Clínica: problemas del día a día»* en I Jornada sobre la Confidencialidad y el Secreto Médico. Organización Médica Colegial (OMC), Comisión de Libertades e Informática (CLI) y Federación de Asociaciones para la Defensa de la Sanidad Pública (FADSP) [fuera de línea]: http://www.cgcom.org/notas_prensa/pdf/05_02_04_sec_med_mesa3.pdf [Consulta: 04/04/2008].

GONZÁLEZ S., P.; LIZÁRRAGA B., E., *et al.* (2004). *«Autonomía del Paciente, Información e Historia Clínica»*. Civitas Ediciones, S. L. Madrid. González T., R.M. (2004): *«El Proceso de Investigación. Bases Conceptuales»*, asigna-

tura de Doctorado: «Metodología y Documentación Científica», Instituto de Ciencias de la Educación, Universidad Politécnica de Madrid. Madrid.

GONZÁLEZ T., R. M. (2004): *«El Proceso de Investigación. Bases Conceptuales»*, asignatura de Doctorado: «Metodología y Documentación Científica», Instituto de Ciencias de la Educación, Universidad Politécnica de Madrid. Madrid.

GOST G., J. (2001). *«Gestión Sanitaria y Tecnologías de la Información»*. Sociedad Española de Informática de la Salud (SEIS)[fuera de línea]: http://www.seis.es/informes/2001/PDF/2Gost.pdf [Consulta: 24/06/2005].

GUERREO E., A. (2008). *«Unificación o Centralización de las Cajas de Salud»* [fuera de línea]: http://www.segurosocialuniversitario.com/articulo_cuatro.htm [Consulta: 23/09/2008].

HEREDIA, N. (2015). *«La política sanitaria del Estado Plurinacional»* en «El cambio a fondo» edición especial quinto aniversario del periódico de circulación nacional Página Siete 19 de abril de 2015.

HERNÁNDEZ M. C., C. (2004). *«La Ley 41/2002 y la Normativa sobre Protección y Tratamiento de Datos de Carácter Personal relativos a la Salud»,* en González S., P., Lizárraga B, E. *et al.* (2004). «Autonomía del Paciente, Información e Historia Clínica». Civitas Ediciones, S. L. Madrid.

HERRÁN O., A. I. (2002). *«El Derecho a la Intimidad en la nueva Ley Orgánica de Protección de Datos Personales»*. Editorial Dykinson, S. L. Madrid.

INDARTE, S. (2012): *«Interoperabilidad»* en *«Manual de salud electrónica para directivos de servicios y sistemas de salud»* Publicación de las Naciones Unidas [en línea]: http://82.98.165.8/jsp/base.jsp?contenido=/jsp/publicaciones/inforseis.jsp&id=5.2&informeid=8&titulo= [Consulta: 18/06/2015].

INDARTE G., S., y VERO S., A (2014). *«Sistemas de apoyo a la toma de decisiones clínicas y de gestión en atención primaria de salud»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud. Volumen II Aplicaciones de las TIC a la atención primaria de salud» Publicación de las Naciones Unidas [en línea]: http://www.seis.es/documentos/X%20Informe%20SEIS%20-%20COMPLETO.pdf [Consulta: 20/03/2015].

INSTITUTO DE ESTUDIOS SUPERIORES DE LA EMPRESA IESE- INTERNATIONAL RESEARCH CENTER ON ORGANIZATIONS IRCO (2002). *«Outsourcing de Recursos Humanos»*.

INSTITUTO DE INFORMACIÓN SANITARIA (2009). *«El Sistema de Historia Clínica Digital del SNS»* [en línea]: http://www.msssi.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf[Consulta: 28/03/2015].

INSTITUTO NACIONAL DE SEGUROS DE SALUD (2008). *«INASES»* [en línea]: http://inases.gob.bo/informacion-institucional-2/politicas-y-estrategias/ [Consulta: 24/01/2015].

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (2010). *«Curso de Sistemas de Gestión de la Seguridad de la Información se-*

gún la norma UNE-ISO/IEC 27000» [en línea]: https://www.academia.edu/8810963/CURSO_DE_SISTEMAS_DE_GESTI%C3%93N_DE_LA_SEGURIDAD_DE_LA_INFORMACI%C3%93N_SEG%C3%9AN_LA_NORMA_UNE-ISO_IEC_27000_INTECO-CERT [Consulta: 08/04/2015].

— (2010). *«Estudio sobre la privacidad y la seguridad de los datos personales en el sector sanitario español»* [en línea]: http://www.inteco.es/file/plLW9PPN9b_MlxpjOX2pMw [Consulta: 11/06/2015].

— (2012). *«Guía sobre riesgos y buenas prácticas en autenticación online»*. Instituto Nacional de Tecnologías de la Comunicación. España.

INSTITUTE OF MEDICINA (2004). *«Patient Safety: Achieving a news Standard for Care»*. National Academy Press [en línea]: http://www.nap.edu/read/10863/chapter/1#xvii [Consulta: 18/06/2015].

INTERNET SOCIETY (2009). *«IPv6 para todos: Guía de uso y aplicación para diversos entornos»*. Internet Society Capítulo Argentina (E-book), Primera Edición octubre 2009, Buenos Aires.

ISACA (2015). *«Glossary of Terms English-Spanish Third edition»*. Information Systems Audit and Control Association [en línea]: http://www.isaca.org/About-ISACA/History/Documents/ISACA-Glossary-English-Spanish_mis_Spa_0415.pdf [Consulta: 30/04/2015].

JACOB, J. (1999). *«Datos objeto de protección especial: Datos de carácter médico-social»*. Agencia de Protección de Datos. Edición XX Conferencia Internacional de Autoridades de Protección de Datos. Madrid, Cit. Sánchez C., C. (2000). «La Intimidad y el Secreto Médico». Ediciones Díaz, S. A. Madrid.

JAÑEZ, F. M.; ZAPATERO, J.; RAMOS, F.; PUENTE, N.; MUÑIZ, N.; SÁNCHEZ-CRESPO, A., y CARRASCO, J. (2002). *«La Protección de datos Personales en el Ámbito Sanitario»*. Editorial Aranzadi, S. A. Navarra.

JOYANES A., L. (2012). *«Computación en la nube. Estrategias de Cloud Computing en las Empresas»*. Alfaomega Grupo Editor, S. A. de C.V., México.

KIM, K. (2005). *«Clinical Data Standards in Health Care: Five Case Stuides»*. Oakland, CA: California Health Care Foundation [en línea]: http://www.chcf.org/publications/2005/07/clinical-data-standards-in-health-care-five-case-studies [Consulta: 20/06/2015].

KLASNJA, P., y PRATT, W. (2012). *«Healthcare in the pocket: mapping the space of mobile-phone health interventions»*, Journal of Biomedical Informatics, vol. 45, N.º 1 [en línea]: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3272165/pdf/nihms323686.pdf [Consulta: 30/04/2015].

LAÍN ENTRALGO, P. (1998). *«La Historia Clínica»*. Triacastela. Madrid.

LA RAZÓN (2014). *«Bolivia exhibirá ante el mundo una appmóvil»* Periódico de circulación nacional [en línea]: http://www.la-razon.com/suplementos/financiero/Bolivia-exhibira-mundo-app-movil-financiero_0_2136986375.html [Consulta: 18/06/2015].

LEDO, C., y SORIA, R. (2011). *«Sistema de salud de Bolivia»* [en línea]: http://www.scielosp.org/pdf/spm/v53s2/07.pdf [Consulta: 12/03/2015].

LEÓN S., P. (2004). *«La Implantación de los Derechos del Paciente»*. Ediciones Universidad de Navarra, S. A. Navarra.

LLANQUE L., G. (2011). *«Análisis del funcionamiento de Programas Verticales en Servicios de Primer Nivel de atención de la Red I de Cercado»* Tesis de la Facultad de Medicina de la Universidad Mayor de San Simón, Cochabamba – Bolivia [en línea]: http://atlas.umss.edu.bo:8080/jspui/bitstream/123456789/116/1/ANALISIS%20DEL%20FUNCIONAMIENTO%20DE%20LOS%20PROGRAMAS%20VERTICALES%20EN%20LOS%20CENTROS%20DE%20SALUD%20DE%201%20ER%20NIVEL.%20DE%20CERCADO,%20GESTION%202011..pdf [Consulta: 02/02/2015].

LÓPEZ C., J. L. (1989). *«Métodos e Hipótesis Científicos»*. Editorial Trillas. México.

LÓPEZ G., J. (2004). *«Antecedentes Históricos y Contexto de la Ley 41/2002»* en León S., P. (2004). «La Implantación de los Derechos del Paciente». Ediciones Universidad de Navarra, S. A. (EUNSA). Navarra.

LÓPEZ G., L. y GISBERT C., J.A. (1998). *«El secreto médico. Confidencialidad e Historia Clínica»*. Medicina Legal y Toxicología, 5.ª Edición, Masson. Madrid, pp. 76, Cit. por De Miguel S., N. (2002). «Secreto Médico, Confidencialidad e Información Sanitaria». Marcial Pons Ediciones Jurídicas y Sociales, S. A. Madrid.

LÓPEZ G., R. (2000). *«La Historia Clínica: Custodia y Propiedad (I)»*, en I Jornadas de Protección de Datos Sanitarios en la Comunidad de Madrid, Agencia de Protección de Datos de la Comunidad de Madrid. Madrid: Editorial MAPFRE, S. A.

LÓPEZ, P.; MOYA, F.; MARIMÓN, S., y PLANAS, I. (2001). *«Protección de Datos de Salud. Criterios y Plan de Seguridad»*. Ediciones Díaz Santos, S. A. Madrid.

Los Tiempos (2014). *«VIH, Tuberculosis y Malaria: Bolivia en riesgo de perder 41 millones de dólares»* [En línea]: http://www.lostiempos.com/oh/actualidad/actualidad/20140712/vih-tuberculosis-y-malaria-bolivia-en-riesgo-de-perder-41-millones-de_266376_583958.html [Consulta: 23/09/2014].

MANNY, C (2003). *«La intimidad de la Unión Europea y la seguridad de los Estados Unidos: la tensión entre la ley europea de protección de datos y los esfuerzos por parte de los Estados Unidos por utilizar los datos sobre pasajeros aéreos para luchar contra el terrorismo y otros delitos»*en «Cuadernos de Derecho Público» 19-20, mayo-diciembre 2003. Edita Instituto Nacional de Administración Pública. Madrid.

MANUNTA, G. (2003). *«Seguridad: Una introducción»*. Revista Seguridad Corporativa y Protección del patrimonio [en línea]: http://www.belt.es/bibliografia/HOME2_articulo.asp?id=130 [Consulta: 16/04/2015].

MARKLE FOUNDATION (2003). *«Connecting for Health –The Personal Health Working Group –Final Report»*, Nueva York [en línea]: http://www.policyarchive.org/handle/10207/bitstreams/15473.pdf [Consulta: 15/06/2015].

MARTÍ M., C. y PIDEVALL B., I. (2004). *«Accesos a la Historia Clínica, con especial referencia a la Disposición Adicional Tercera de la Ley 41/2002 y al Artículo 11.5 referente al Acceso a las Instrucciones Previas»*, en «Autonomía del Paciente, Información e Historia Clínica». Civitas Ediciones, S. L. Madrid. Pp. 101-136.

MARTÍN-CASALLO L., J. J. (2001). *«Derechos de Acceso, Rectificación y Cancelación de los Datos Sanitarios en la LOPD»*. VII Congreso Nacional de Derecho Sanitario, Ediciones Fundación MAPFRE Medicina, pág. 58, Cit. Sánchez-Caro y Abellán (2004) «Datos de Salud y Datos Genéticos». Editorial Comares, S. L. Granada.

MARTÍNEZ DEL CERRO, F. J. (2004). *«Nuevas Tecnologías: Historia Clínica Electrónica y Telemedicina»,* en Ruiz I., L. (2004). *«Claves para la Gestión Clínica»*. McGraw-Hill/Interamericana de España, S. A. U. Madrid.

MARTÍNEZ N., A. (2001). *«La Ley Española de Firma Electrónica (RD Ley14/1999)»*, en «Derecho del Comercio Electrónico». Edita La Ley. Madrid.

— (2014). *«Comentarios a la Ley 59/2003 de Firma Electrónica»*. Editorial Civitas, S. L.

MARTÍNEZ, S. y ROJAS DE LA ESCALERA, D. (2014). *«Gestión de la seguridad de la información en atención primaria y uso responsable de Internet y de las redes sociales»* en Manual de Salud Electrónica para directivos de servicios y sistemas de salud. Volumen II Aplicaciones de las TIC a la atención primaria de salud» Publicación de las Naciones Unidas [en línea]: http://www.seis.es/documentos/X%20Informe%20SEIS%20-%20COMPLETO.pdf [Consulta: 20/03/2015].

MAZÓN, P., y CARNICERO, J. (2001). *«La informatización de la documentación clínica: oportunidad de mejora de la práctica clínica y riesgos para la seguridad y confidencialidad»*. Sociedad Española de Informática de la Salud (SEIS) [en línea]:http://82.98.165.8/jsp/base.jsp?contenido=/jsp/publicaciones/inforseis.jsp&id=5.2&informeid=1&titulo= [Consulta: 28/04/2015].

MEDICUS MUNDI DELEGACIÓN BOLIVIA (2006). *«Sistema de Información Clínico Estadístico»*. Editorial Publicidad e Impresión Génesis, La Paz.

— (2006). *«Sistema Integrado de Administración Financiera»*. Editorial Publicidad e Impresión Génesis, La Paz.

MÉDICOS Y PACIENTES (2010). *«Entrevista con el director del Observatorio del Sistema Nacional de Salud, el doctor Javier Carnicero»* [en línea]: http://historico.medicosypacientes.com/noticias/2010/03/10_03_09_entrevista [Consulta: 08/04/2015].

MEDINACELI D., K. (2004). *«El outsourcing clave de éxito en la empresa actual»* Libro de comunicaciones de la I Jornada Académica de Postgrado de

Investigación en Ingeniería Informática de la UPSA, Salamanca, 2004. ISBN: 84-688-6550-8.

— (2015). *«La seguridad de la información clave en la protección de datos sanitarios» Revista de la Biblioteca y Archivo Histórico de la Asamblea Legislativa Plurinacional,* Año 14, Volumen 9, Número 38, junio 2015, ISSN 2225-3769 – D.L. 4-3-96-02.

MEJICA G., J., y DÍEZ R., J. R. (2006). *«El Estatuto del Paciente a través de la nueva legislación sanitaria estatal»*. Editorial Aranzadi, S. A. Navarra.

MELAMUD, A., y OTERO, P. (2011). *«Facebook y Twitter ¿están ya en el consultorio de los pediatras?»* Encuesta sobre el uso de la redes sociales [en línea]: http://www.scielo.org.ar/scielo.php?pid=S032500752011000500011&script=sci_arttext [Consulta: 18/06/2015].

MIFSUD, E. (2012). *Introducción a la seguridad informática* [en línea]: http://recursostic.educacion.es/observatorio/web/es/component/content/article/31-general/1040-introduccion-a-la-seguridad-informatica?format=pdf [Consulta: 08/05/2015].

MINISTERIO DE SALUD (2015): *«Código de Ética y Deontología Médica»* [en línea]: http://www.minsalud.gob.bo/images/Documentacion/normativa/CODIGODEETICAYDEONTOLOGIAMEDICA.pdf [Consulta: 28/01/2015].

— (2015): *«Comité Técnico-Consejo Nacional de Alimentación y Nutrición/ Programa Multisectorial Desnutrición Cero»* [en línea]: http://www.ctconan.minsalud.gob.bo/ct_conan.php [Consulta: 09/01/2015].

— (2015): *«Delimitación de territorio»* [en línea]: http://snis.minsalud.gob.bo/index.php?ID=Delimitaciones [Consulta: 09/01/2015].

— (2015): *«Estructura estatal de salud: rol y funciones en la gestión compartida de la salud»* [en línea]: http://snis.minsalud.gob.bo/index.php?ID=Estrucestatal [Consulta: 09/01/2015].

— (2015): *«Estructuras y Actores que intervienen en la gestión compartida»* [en línea]: http://snis.minsalud.gob.bo/index.php?ID=Estrucyactores [Consulta: 09/01/2015].

— (2015): *«La salud en el Plan Nacional de Desarrollo»* [en línea]: http://www.ine.gob.bo/indicadoresddhh/archivos/salud/nal/Plan%20Sectorial%20de%20Desarrollo%202010-2020.pdf [Consulta: 17/01/2015].

— (2015): *«Oruro celebra primer año de la implementación del programa Mi Salud»* [en línea]: http://www.minsalud.gob.bo/645-oruro-celebra-primer-implementacion [Consulta: 19/06/2015].

— (2015): *«Plan Sectorial de Desarrollo»* [en línea]: http://www.ine.gob.bo/indicadoresddhh/archivos/salud/nal/Plan%20Sectorial%20de%20Desarrollo%202010-2020.pdf [Consulta: 28/01/2015].

— (2015): *«Política 1 Sistema Único, Intercultural y Comunitario de Salud»* [en línea]: http://www.ine.gob.bo/indicadoresddhh/archivos/salud/nal/Plan%20Sectorial%20de%20Desarrollo%202010-2020.pdf [Consulta: 17/01/2015].

— (2015): *«Política 2 Rectoría»* [en línea]: http://www.ine.gob.bo/indicadoresddhh/archivos/salud/nal/Plan%20Sectorial%20de%20Desarrollo%202010-2020.pdf [Consulta: 17/01/2015].

— (2015): *«Política 3 Movilización sectorial»* [en línea]: http://www.sns.gov.bo/viceministerio/deportes/promoción_salud/salud_comunitaria/delimitacion [Consulta: 09/01/2015].

— (2015): *«Política 4 Promoción de la Salud»* [en línea]: http://www.sns.gov.bo/viceministerio/deportes/promoción_salud/salud_comunitaria/delimitacion [Consulta: 09/01/2015].

— (2015): *«Política 5 Solidaridad»* [en línea]: http://www.sns.gov.bo/viceministerio/deportes/promoción_salud/salud_comunitaria/delimitacion [Consulta: 09/01/2015].

— (2015): *«Políticas y Estrategias»* [en línea]: http://www.ine.gob.bo/indicadoresddhh/archivos/salud/nal/Plan%20Sectorial%20de%20Desarrollo%202010-2020.pdf [Consulta: 17/01/2015].

— (2015): *«Primer Nivel de Complejidad»* [en línea]: http://snis.minsalud.gob.bo/index.php?ID=Aplicacionatencion [Consulta: 09/01/2015].

— (2015): *«Programa SAFCI. Filosofía»* [en línea]: http://www.rm-safci.gob.bo/index.php/institucional/filosofia [Consulta: 09/01/2015].

— (2015): *«Salud Familiar Comunitaria Intercultural»* [en línea]: http://www.ine.gob.bo/indicadoresddhh/archivos/salud/nal/Plan%20Sectorial%20de%20Desarrollo%202010-2020.pdf [Consulta: 15/01/2015].

— (2015): *«Segundo Nivel de Complejidad»* [en línea]: http://snis.minsalud.gob.bo/index.php?ID=Aplicacionatencion [Consulta: 09/01/2015].

— (2015). *«Telesalud Bolivia: tecnologías para los bolivianos»*, Boletín Informativo agosto de 2015, La Paz-Bolivia.

— (2015): *«Tercer Nivel de Complejidad»* [en línea]: http://snis.minsalud.gob.bo/index.php?ID=Aplicacionatencion [Consulta: 09/01/2015].

MINISTERIO DE SALUD Y DEPORTES (2005). *«Código de Ética y Deontología»* Resolución Ministerial N.º 0071 de fecha 17 de febrero de 2005.

— (2005). Resolución Ministerial N.º 0853 de fecha 18 de noviembre de 2005.

— (2008). Resolución Ministerial N.º 0090 de fecha 26 de febrero de 2008 aprueba el *«Manual de Auditoría y Norma Técnica»*.

— (2008). Resolución Ministerial N.º 0090 de fecha 26 de febrero de 2008 aprueba la *«Norma Técnica para el manejo del Expediente Clínico»*.

— (2008). Resolución Ministerial N.º 0090 de fecha 26 de febrero de 2008 aprueba la *«Obtención del Consentimiento Informado»*.

— (2008): *«Sistema Nacional de Información en Salud y Vigilancia Epidemiológica SNIS VE»* [en línea]: http://snis.minsalud.gob.bo/snis/default.aspx [Consulta: 07/01/2015].

— (2010): *«Plan Sectorial de Desarrollo 2010-2020: Hacia la salud universal»* Primera Edición [en línea]: http://www.ine.gob.bo/indicadoresddhh/archivos/salud/nal/Plan%20Sectorial%20de%20Desarrollo%202010-2020.pdf [Consulta: 09/01/2015].

— (2010). *«Propuesta de reestructuración del Sistema nacional de Información en Salud»*, Sistema Nacional de Información en Salud, La Paz-Bolivia.

— (2012). *«Manual de procesos y procedimientos para la gestión de información de producción de servicios de I nivel de atención»*, Sistema Nacional de Información en Salud, La Paz-Bolivia.

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD (2009). *«Sistema de Historia Clínica Digital del Sistema Nacional de Salud»* elaborado por el Instituto de Información Sanitaria [en línea]:http://www.msssi.gob.es/profesionales/hcdsns/home.htm [Consulta: 18/05/2015].

— (2012): *«Manual de Procedimientos para el reconocimiento de Registros, Encuestas y Sistemas de Información de utilidad para el Sistema Nacional de Salud»* [en línea]: http://www.msssi.gob.es/estadEstudios/estadisticas/sisInfSanSNS/pdf/MANUAL_DE_PROCEDIMIENTOS_RRSISNS.pdf [Consulta: 08/04/2015].

— (2015): *«Historia Clínica Digital en el Sistema Nacional de Salud (SNS). Contenido de la Historia Clínica Digital del SNS»* [en línea]: http://www.msssi.gob.es/profesionales/hcdsns/contenidoDoc/contenidos.htm [Consulta: 20/03/2015].

— (2015): *«Historia Clínica Digital en el Sistema Nacional de Salud (SNS). Contexto General»* [en línea]: http://www.msssi.gob.es/profesionales/hcdsns/contenidoDoc/contexto.htm [Consulta: 20/03/2015].

— (2015): *«Historia Clínica Digital en el Sistema Nacional de Salud (SNS). Diseño funcional»* [en línea]: http://www.msssi.gob.es/profesionales/hcdsns/contenidoDoc/disenoFunc.htm [Consulta: 20/03/2015].

— (2015): *«Historia Clínica Digital en el Sistema Nacional de Salud (SNS). Objetivos generales»* [en línea]: http://www.msssi.gob.es/profesionales/hcdsns/contenidoDoc/objetivos.htm [Consulta: 20/03/2015].

— (2015): *«Sanidad en Línea Fase I»* [en línea]: http://www.red.es/redes/actuaciones/sanidad-en-linea/sanidad-en-linea-fase-i [Consulta: 20/03/2015].

MI SALUD (2014). *«Telesalud. La tecnología al servicio de la salud»* Revista Mensual año 1 / N.º 4 2014, Ministerio de Salud, La Paz-Bolivia.

MOLET, J. (2015). *«Las 5 claves para cumplir con la Ley Federal de Protección de Datos Personales por parte de las empresas»* [en línea]: http://www.proteccionde datospersonales.org/2015/01/23/las-5-claves-para-cumplir-con-la-ley-federal-de-proteccion-de-datos-personales-por-parte-de-las-empresas/#_ftn2 [Consulta: 10/05/2015].

MONTEAGUDO P., J. L. (2004). *«El Marco de las Nuevas Tecnologías»*en Ruiz I., L. (2004). «Claves para la Gestión Clínica».McGraw-Hill/Interamericana de España, S. A. U. Madrid.

MORENO V., M. (2002). *«Documentación clínica: organización, custodia y acceso»* en «La Historia Clínica». Editorial COMARES, S. L. Granada.

MOURA, L.; INDARTE, S., y DE FARIA LEÓN, B. (2014). *«La necesidad de una arquitectura de salud-e»* en Manual de Salud Electrónica para directivos de servicios y sistemas de salud. Volumen II Aplicaciones de las TIC a la atención primaria de salud» Publicación de las Naciones Unidas [en línea]: http://www.seis.es/documentos/X%20Informe%20SEIS%20-%20COMPLETO.pdf [Consulta: 20/03/2015].

MURILLO DE LA CUEVA, L. (1990). *«El Derecho a la Autodeterminación Informativa. La protección de los datos personales frente al uso de la informática»*. Editorial TECNOS, S. A. Madrid.

— (1997). *«El tratamiento jurídico de los documentos y registros sanitarios informatizados y no informatizados»*. Seminario Conjunto sobre Información y Documentación Clínica, Consejo General del Poder Judicial y Ministerio de Sanidad y Consumo. Madrid: Ministerio de Sanidad y Consumo, Vol. II.

NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY (2011). *«The NIST Definition of Cloud Computing»* [en línea]: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [Consulta: 15/06/2015].

OBSERVATORIO NACIONAL PARA LAS TELECOMUNICACIONES Y LA SOCIEDAD DE LA INFORMACIÓN (2012). *«Los ciudadanos ante la e-Sanidad»* Ministerio de Industria, Energía y Turismo [en línea]: http://www.ontsi.red.es/ontsi/sites/default/files/informe_ciudadanos_esanidad.pdf [Consulta: 20/06/2015].

OPORTO, H. (2014). *«La reforma sanitaria pendiente»* en «Bolivia encrucijadas en el siglo XXI» Editora Presencial SRL, La Paz.

ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA EDUCACIÓN, LA CIENCIA Y CULTURA (2003). *«Declaración Universal sobre el Genoma Humano y Derechos Humanos de fecha 11 de noviembre de 1997»* [en línea]: http://portal.unesco.org/es/ev.php-URL_ID=13177&URL_DO=DO_TOPIC&URL_SECTION=201.html[Consulta: 23/06/2014].

— (2003). *«Declaración Internacional sobre los Datos Genéticos Humanos de fecha 16 de octubre de 2003»*[en línea]: http://portal.unesco.org/es/ev.php-URL_ID=17720&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html[Consulta: 23/06/2014].

ORGANIZACIÓN MÉDICA COLEGIAL *et al.* (2005). *«Conclusiones»* en I Jornada sobre la Confidencialidad y el Secreto Médico. Organización Médica Colegial (OMC), Comisión de Libertades e Informática (CLI) y Federación de Asociaciones para la Defensa de la Sanidad Pública (FADSP) [en línea]: http://www.cgcom.es/noticias/2005/02/05_02_07_secreto_medico [Consulta: 04/04/2015].

ORGANIZACIÓN MUNDIAL DE LA SALUD (1990). *«La intervención de la comunidad en el desarrollo sanitario: examen de los aspectos esenciales»* [en línea]: http://apps.who.int/iris/handle/10665/39398 [Consulta: 08/04/2015].

— (2011). *«New horizons for health through mobile technologies»* Global Observatory for eHealth Series, vol. 3, Ginebra [en línea]: http://www.who.int/goe/publications/goe_mhealth_web.pdf [Consulta: 18/06/2015].

ORGANIZACIÓN PANAMERICANA DE LA SALUD (2004). *«Caracterización de la exclusión en salud en Bolivia»* [en línea]: http://www.udape.gob.bo/portales_html/exclusion/Caracterizaci%C3%B3n%20de%20la%20Exclusi%C3%B3n%20en%20Salud%20en%20Bolivia.pdf [Consulta: 12/03/2015].

ORGANIZACIÓN PANAMERICANA DE LA SALUD-BOLIVIA (2007). *«VIH/SIDA, Gobierno y Fondo Mundial: cuestión de vida»* [fuera de línea]: http://www.ops.org.bo/cgi/sys/s2a.xic?DB=B&S2=2&S11=12911&S22=b [Consulta: 07/10/2008].

— (2008): *«Estadísticas de VIH/SIDA: Datos de Bolivia 1984 - 2003»* [fuera de línea]: http://www.ops.org.bo/its-vih-sida/?TE=20040628161715 [Consulta: 01/10/2008].

PÁGINA SIETE (2015). *«Arco Iris inaugura su centro de salud en la zona Sur»* periódico de circulación nacional [en línea]: http://www.paginasiete.bo/sociedad/2015/9/29/arco-iris-inaugura-centro-salud-zona-71696.html [Consulta: 30/09/2015].

— (2015). *«Decreta, 8,5% de incremento y el salario mínimo sube a 1.656»* [en línea]: http://www.paginasiete.bo/nacional/2015/5/2/decretan-85-incremento-salario-minimo-sube-1656-55315.html [Consulta: 25/09/2015].

— (2015). *«Hospital Boliviano Holandés será exclusivamente materno-infantil»* [en línea]: http://www.paginasiete.bo/sociedad/2015/11/5/hospital-boliviano-holandes-sera-exclusivamente-materno-infantil-75885.html [Consulta: 25/09/2015].

— (2015). *«La mujer que organizó el archivo clínico militar»* Periódico de circulación nacional, domingo 2 de agosto de 2015 [en línea]: http://www.paginasiete.bo/gente/2015/8/2/mujer-reorganizo-archivo-clinico-militar-65166.html [Consulta: 29/09/2015].

PALOMARES B., M.; LÓPEZ Y GARCÍA, J., *et al.* (2002). *«El consentimiento informado en la práctica médica y el testamento vital»*. Editorial COMARES, S. L.

PERALES G., P. (2004). *«El Hábeas Data. Bolivia en el Constitucionalismo Iberoamericano»*. Edición Talleres Gráficos Gaviota del Sur, S.R.L. Sucre.

PÉREZ CAMPANERO, J. A. (2001). *«La gestión de seguridad en los sistemas de información y de las comunicaciones»*. Sociedad Española de Informática de la Salud (SEIS) [en línea]: http://www.conganat.org/SEIS/informes/2001/PDF/5PerezCampanero.pdf [Consulta: 24/04/2015].

PÉREZ-ÍÑIGO Q., F., y ABARCA C., J. (2001). *«Un Modelo de Hospital»*. Medicina stm Editores, S. L. Barcelona.

PIERINI, A.; LORENCES, V., y TORNABÉ, M. I. (1999). *«Hábeas Data, Derecho a la Intimidad»*. Editorial Universidad. Buenos Aires, Cit. Perales G., P. (2004). *«El Hábeas Data. Bolivia en el Constitucionalismo Iberoamericano»*. Edición Talleres Gráficos Gaviota del Sur, S.R.L. Sucre.

PLAN AVANZA 2 (2010). *«Las TIC en el Sistema Nacional de Salud. El Programa Sanidad en Línea»* Ministerio de Sanidad y Política Social y Ministerio de Industria, Turismo y Comercio [en línea]: http://www.msssi.gob.es/profesionales/hcdsns/TICS/TICS_SNS_ACTUALIZACION_ES_2010.pdf [Consulta: 24/06/2015].

POISSANT, L., y otros (2005). *«The Impact of Electronic Health Records on Time Efficiency of Physicians and Nurses: a Systematic Review»*, J Am Med Inform Assoc, vol. 13, N.º 3 citado por González B., F. y Luna, D. (2012): *«La historia electrónica»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud». Publicación de las naciones Unidas enero de 2012 [en línea]: http://repositorio.cepal.org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 22/03/2015].

PROTTO, J. P., *et al.* (2008). *«Entorno epidemiológico y respuesta a la epidemia del VIH en Bolivia»* [en línea]: http://www.scielosp.org/pdf/rpsp/v23n4/v23n4a12.pdf [Consulta: 06/10/2014].

PUENTE E., A. (2004). *«El Tratamiento de Datos en las Historias Clínicas. La Ley 41/2002, de 14 de noviembre»*. Sociedad Española de Informática de la Salud (SEIS), *Revista Informática y Salud*, Número 47, Junio de 2004 [fuera de línea]: http://www.seis.es/is/is47/IS47_31.pdf [Consulta: 10/07/2005].

RED DE PERSONAS QUE VIVEN CON EL VIH EN BOLIVIA (2015). *«Sistematización Plan de Incidencia Política de REDBOL 2012-2014 para la asignación de recursos en VIH»*. Impresiones Gráficas, Primera Edición. Bolivia.

REIG R., J.; MONTEAGUDO P., J. L., y SPEILBERG B., T. M. (2003). *«La Historia de Salud Electrónica: Perspectiva Internacional»*. Sociedad Española de Informática de la Salud (SEIS)[fuera de línea]: http://www.conganat.org/SEIS/informes/2003/PDF/INDICE.pdf [Consulta: 20/04/2015].

REMOLINA A., N. (2013). *«Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012»*. Legis Editores, S. A. Impreso en Colombia.

REYNALES L., J. (2008). *«Sistema de información hospitalario»* en «Administración Hospitalaria». Editorial Médica Panamericana. Bogotá.

RICUR, G. (2012). *«Telemedicina: generalidades y áreas de aplicación clínica»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud» Publicación de las Naciones Unidas [en línea]: http://82.98.165.8/jsp/base.jsp?contenido=/jsp/publicaciones/inforseis.jsp&id=5.2&informeid=8&titulo= [Consulta: 20/06/2015].

RILEY, W. T., y otros (2011). *«Health behavior models in the age of mobile interventions: are our theories up to the task?»* Translational Behavioral Medicine, vol. 1, N.º 1 [en línea]: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3142960/pdf/13142_2011_Article_21.pdf [Consulta: 16/06/2015].

RIMASSA, M.; PÉREZ, G., y TRUJILLO, L. (2007). *«Heterosexualidad y conductas de riesgo»*. Diakonia febrero 2007 [en línea]: http://www.academia.edu/4270980/Heterosexualidad_y_conductas_de_riesgo [Consulta: 06/10/2014].

RIVA, G., y otros (2011). *«Personal health systems for mental health: the European projects»* Studies in Health Technology and Informatics, N.º 163 citado por Curioso V, W. (2014). *«Salud móvil en atención primaria»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud. Volumen II Aplicaciones de las TIC a la atención primaria de salud» Publicación de las Naciones Unidas [en línea]: http://www.seis.es/documentos/X%20Informe%20SEIS%20-%20COMPLETO.pdf [Consulta: 10/06/2015].

RIVERA S., J. A. (2004). *«Jurisdicción Constitucional. Procesos Constitucionales en Bolivia»*. Ediciones Kipus, 2da. Edición. Cochabamba.

— (2010) *«Acción de Protección de Privacidad»* [en línea]: http://www.econstitucional.com/ensayos/Acci%C3%B3n%20de%20protecci%C3%B3n%20de%20privacidad%20J.%20Rivera.pdf [Consulta: 20/10/2014].

RIVERA S., J. A.; JOST, S.; MOLINA R., G., y CAJÍAS, H. J. (2005). *«La Constitución Política del Estado. Comentario Crítico»*. Editado por Fundación Konrad Adenauer, 3ra. Edición, La Paz.

RODRÍGUEZ A., A. (2004). *«Firma Electrónica y Documento Electrónico»*. Edita Consejo General del Notariado. Madrid.

RODRÍGUEZ L., P. (2004). *«La Autonomía del Paciente. Información, Consentimiento y Documentación Clínica»*. Editorial Dilex, S. L. Madrid.

RODRÍGUEZ S., J. J. (2005). *«Consideraciones sobre el Secreto Profesional Médico»*, en I Jornada sobre la Confidencialidad y el Secreto Médico. Organización Médica Colegial (OMC), Comisión de Libertades e Informática (CLI) y Federación de Asociaciones para la Defensa de la Sanidad Pública (FADSP) [en línea]: http://www.semg.es/documentos-semg/opinion/409-consideraciones-sobre-el-secreto-profesional-medico.html [Consulta: 04/04/2015].

ROJAS, D.; MARTÍNEZ, R., y ELICEGUI, I. (2012). *«Infraestructura y requisitos básicos de los sistemas de salud electrónica»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud». Publicación de las Naciones Unidas enero de 2012 [en línea]: http://repositorio.cepal.org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 22/03/2015].

ROJAS, D., y BLANCO, O. (2008). *«Requisitos de seguridad de la información del sector sanitario»*. Sociedad Española de Informática de la Salud (SEIS) y Navarra de Gestión para la Administración (NGA). Pamplona [en línea]: http://www.seis.es/documentos/informes/secciones/adjunto1/Capitulo_3_Re-

quisitos_de_seguridad_de_la_informacion_del_sector_sanitario.pdf[Consulta: 03/05/2015].

ROJO V., P. (2007). «*Tecnología de la información*». Edición DM. Murcia.

ROMEO C., C. M. (2002). «*Los Genes y sus Leyes. El Derecho ante el Genoma Humano*». Editorial Comares, S. L. Granada.

ROMEO C., C. M., y CASTELLANO A., M. (2002). «*La intimidad del paciente desde la perspectiva del secreto médico y del acceso a la historia clínica*», en Derecho y Salud, vol. 1 nú.1, julio a diciembre 1993, págs. 8 y ss., citado por Mejica G., J. y Díez R., J.R. (2006). «*El Estatuto del Paciente a través de la nueva legislación sanitaria estatal*». Editorial Aranzadi, S. A. Navarra.

ROMERO C., A. M. (2002). «*La medicina antes los derechos del paciente*». Editorial Montecorvo, S. A. Madrid.

ROMERO G., A. (2004). «*Sistemas de Información para la Gestión de un Servicio*», en Ruiz I., L. (2004). «*Claves para la Gestión Clínica*». McGraw-Hill/Interamericana de España, S. A. U. Madrid.

ROSADO, E. (2004). «*El futuro ha llegado a la gestión del SESCAM*» [en línea]: http://www.jccm.es/revista/163/articulos163/afondo_marzo.htm [Consulta: 11/08/2008].

ROSELLO M., R. (2001). «*El comercio electrónico y la protección del consumidor*». Centro de Estudios de Derecho, Economía y Ciencias Sociales - Cedecs Editorial, S. L., Barcelona.

RUBÍ N., J. (2000). «*Los Código Tipo: la alternativa de la autorregulación*». Revista Actualidad Informática Aranzadi, Número 35, abril de 2000, Cit. Sánchez-Caro, J. y Abellán, F. (2004). «*Datos de Salud y Datos Genéticos*». Editorial Comares, S. L. Granada.

— (2004): «*La confidencialidad de la información sanitaria, instrumento de protección y garantía*» en «La salud como valor constitucional y sus garantías». Edita Defensor del Paciente de la Comunidad de Madrid.

RUIZ C., A. (2005). «*Manual Práctico de Protección de Datos*». Editorial Bosch, S. A. Barcelona.

— (2008). «*El Tratamiento de los datos personales en los documentos de seguridad*». Editorial Bosch, S. A. Barcelona.

RUIZ I., L. (2004). «*Claves para la Gestión Clínica*». McGraw-Hill/Interamericana de España, S. A. U. Madrid.

RUIZ M., C. (2004). «*El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea*» en «Temas de Direito da Informatica e da Internet». Coimbra Editora. Coimbra.

RUIZ T., A. (2005). «*Confidencialidad y Modelo de Informatización*», en I Jornada sobre la Confidencialidad y el Secreto Médico. Organización Médica Colegial (OMC), Comisión de Libertades e Informática (CLI) y Federación de Asociaciones para la Defensa de la Sanidad Pública (FADSP) [fuera de lí-

nea]: http://www.cgcom.es/noticias/2005/02/05_02_14_confidencialidad [Consulta: 04/04/2015].

RUSQUE, A. M. (2003). *«De la Diversidad a la Unidad en la Investigación Cualitativa»*. Vadell Hermanos Editores. Caracas.

SALCEDO B., M. C. (2006). *«La adopción de medidas de vigilancia de la salud por parte del empresario» en* «La salud: intimidad y libertades informativas». Tirant lo Blanch. Valencia.

SÁNCHEZ-CARO, J. (2004). *«Intimidad, Salud y Constitución»* en «La Salud como Valor Constitucional y sus Garantías», Consejería de Sanidad y Consumo de la Comunidad de Madrid [en línea]: http://www.listadeesperamadrid.com/defensor/pdf/lasaludvalorconstitucional.pdf [Consulta: 23/06/2014].

SÁNCHEZ-CARO, J. y ABELLÁN, F. (2002). *«Telemedicina y Protección de Datos Sanitarios»*. Editorial Comares, S. L. Granada.

— (2003). *«Derechos y Deberes de los Pacientes. Ley 41/2002 de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas»*. Editorial Comares, S. L. Granada.

— (2004). *«Datos de Salud y Datos Genéticos»*. Editorial Comares, S. L. Granada.

SÁNCHEZ C., C. (1999). *«Protección de datos de carácter personal relativos a la salud»*. Edita Agencia Española de Protección de Datos. Madrid.

— (2000). *«La Intimidad y el Secreto Médico»*. Ediciones Díaz S. A. Madrid.

SANCHÉZ P., J. M. (2006). *«El régimen jurídico europeo aplicable a la confidencialidad de los datos relativos a la salud de las personas» en* «La salud: intimidad y libertades informativas». Tirant lo Blanch. Valencia.

SANCHO V., D. (2003). *«Transferencia internacional de datos personales»*. Edita Agencia Española de Protección de Datos. Madrid.

SAN JULIÁN P., V. (2004). *«Los Principios Generales de la Ley 41/2002»* en León S., P. (2004). «La Implantación de los Derechos del Paciente». Ediciones Universidad de Navarra, S. A. Navarra.

SANZ, J., y HUALDE, S. (2001). *«Aspectos técnicos de la seguridad en la información sanitaria»*. En La Seguridad y confidencialidad de la información clínica. Sociedad Española de Informática de la Salud (SEIS). Pamplona.

STAUSBERG, J., y otros (2003). *«Comparing Paper-based with Electronic Patient Records: Lessons Leraned during a Study on Diagnosis and Procedure Codes»*, J Am Med Inform Assoc, vol. 10, N.º 5 citado por González B., F. y Luna, D. (2012): *«La historia electrónica»* en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud». Publicación de las naciones Unidas enero de 2012 [en línea]: http://repositorio.cepal.org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 22/03/2015].

SEGURO SOCIAL UNIVERSITARIO (2008). *«Seguro Social Universitario Santa Cruz de la Sierra Bolivia»* [en línea]: http://www.ssusrz.org/web/index.php/component/content/?view=featured [Consulta: 23/01/2015].

— (2015). «*Seguro Social Universitario de La Paz*» [en línea]: http://www.ssulapaz.org/historia.html [Consulta: 23/01/2015].

SEOANE, J. A. (2004). «*El Significado de la Ley Básica de Autonomía del Paciente (Ley 41/2002, de 14 de noviembre) en el Sistema Jurídico-Sanitario Español. Una propuesta de interpretación*», Revista Derecho y Salud, Número 12, Enero–Junio de 2004 [fuera de línea]: http://www.ajs.es/RevistaDS/Vol12-04.pdf [Consulta: 10/07/2005].

SERRANO P., M. M. (2003). «*El Derecho Fundamental a la Protección de Datos. Derecho español y comparado*». Civitas Ediciones, S. L. Madrid.

SERVICIO DEPARTAMENTAL DE LA PAZ (2008). «*Directorios Locales de Salud: propuesta renovada de gestión y participación social en salud para el Departamento de La Paz*». Impresión Garza Azul Impresores & Editores, La Paz.

SERVICIO DEPARTAMENTAL DE SALUD (2015). «*Antecedentes Históricos del SEDES La Paz*» [en línea]: http://www.sedeslapaz.gob.bo/index.php?option=com_content&view=article&id=19&Itemid=27 [Consulta: 12/01/2015].

— «*Centros de vigilancia, información y referencia-CVIR La Paz*» Programa Departamental ITS/VIH/SIDA [en línea]: http://www.sedeslapaz.gob.bo/index.php?option=com_content&view=article&id=114:psida&catid=41:peer&Itemid=112 [Consulta: 06/06/2015].

SEVY, C. (2015). «*Cloud Computing en sector salud*» [en línea]: https://carlossevy.wordpress.com/2015/07/06/cloud-computing-en-sector-salud/ [Consulta: 12/09/2015].

SIMON, S. R., y otros (2007). «*Physicians and Electronic Helath Records: a Statewide Survey*», Arch Intern Med, vol. 167, N.º 5 citado en González B., F. y Luna, D. (2012): «*La historia electrónica*» en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud». Publicación de las naciones Unidas enero de 2012 [en línea]: http://repositorio.cepal.org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 22/03/2015].

SISTEMA NACIONAL DE INFORMACIÓN EN SALUD (2010). «*Sistema Integrado de Administración Financiera-SIAF*», La Paz-Bolivia.

SOCIEDAD ANDALUZA DE MEDICINA FAMILIAR Y COMUNITARIA (2008): «*Conclusiones Foro Diraya*» [en línea]: http://www.samfyc.es/modules/Convocatorias/condiraya.pdf [Consulta: 10/08/2008].

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD (2003). «*V Informe. De la historia clínica a la historia de salud electrónica*» [fuera de línea]: http://www.seis.es/informes/2003/ [Consulta: 10/06/2005].

SOUTHER, E. (2001). «*Implementation of the Electronic Medical Record: the Team Approach*», Comput Nurs, vol.10 N.º 2 citado por González B., F. y Luna, D. (2012): «*La historia electrónica*» en «Manual de Salud Electrónica para directivos de servicios y sistemas de salud». Publicación de las naciones

Unidas enero de 2012 [en línea]: http://repositorio.cepal.org/bitstream/handle/11362/3023/S2012060_es.pdf?sequence=1 [Consulta: 22/03/2015].

TAMAYO T., M. (1996). *«El proceso de la investigación científica»*, Limusa, Noriega Editores, 4ta edición, México.

TANG, P. C., y otros (2003). *«Key Capabilities of an Electronic Health Record System: Letter Report»* Washington, DC: Institute of Medicine. National Academy Press [en línea]: http://www.nap.edu/read/10781/chapter/1 [Consulta: 15/06/2015].

— (2006). *«Personal health reocrds: definitions, benefits and strategies for overcoming barriers to adoption»*, Journal of the American Medical Informatics Association, vol. 13, N.º 2 [en línea]: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1447551/pdf/121.pdf [Consulta: 20/06/2015].

TECNOLOGÍA, INNOVACIÓN I SALUT (2013). *«La Comisión Europea diagnostica el estado de la eSalud en Europa con dos nuevos análisis comparativos»* Generalitat de Catalunya Departament de Salut [en línea]: http://www.ticsalut.cat/actualitat/es_noticies/seccio/58/53/la-comision-europea-diagnostica-el-estado-de-la-esalud-en-europa-con-dos-nuevos-analisis-comparativos [Consulta: 22/06/2015].

TÉLLEZ A., A. (2002). *«La Protección de Datos en la Unión Europea»*. Edita EDISOFER, S. L. Madrid.

TÉLLEZ V., J. (2005). *«Derecho Informático»*. McGraw-HILL/INTERAMERICANA Editores, S. A., de C.V. México.

TOMAS-VALIENTE, L., C., García R., Y., *et al.* (2006). *«La salud: intimidad y libertades informativas»*. Tirant lo Blanch. Valencia.

TRIBUNAL CONSTITUCIONAL PLURINACIONAL (2003). «Sentencia Constitucional 01743/2003-R» de fecha 01 de diciembre de 2003 [en línea]: https://buscador.tcpbolivia.bo/%28S%28pwo4tl0pa5khqiu5hfsk0u0r%29%29/WfrJurisprudencia.aspx [Consulta: 23/03/2015].

— (2006). *«Sentencia Constitucional 0030/2006-R»* de fecha 11 de enero de 2006.

— (2010). *«Sentencia Constitucional 0189/2010-R»* de fecha 24 de mayo de 2010 [en línea]: https://buscador.tcpbolivia.bo/%28S%28xp2bbzln5se1xifd4hzvg3zw%29%29/WfrJurisprudencia.aspx [Consulta: 23/03/2015].

— (2010). *«Sentencia Constitucional 01738/2010-R»* de fecha 25 de octubre de 2010 [en línea]: https://buscador.tcpbolivia.bo/%28S%28xp2bbzln5se1xifd4hzvg3zw%29%29/WfrJurisprudencia.aspx [Consulta: 23/03/2015].

— (2011). *«Sentencia Constitucional 1978/2011-R»* de fecha 7 de diciembre de 2011 [en línea]: http://buscador.tcpbolivia.bo/%28S%28pop2ffjidnb0ghsgjvksxrj1%29%29/WfrJurisprudencia.aspx [Consulta: 23/03/2015].

— (2013). *«Sentencia Constitucional 0851/2013-L»* de fecha 14 de agosto de 2013 [en línea]: https://buscador.tcpbolivia.bo/%28S%280hq5u0lzpaeb4xb4z1ubv3hd%29%29/WfrJurisprudencia.aspx [Consulta: 23/03/2015].

— (2014). «Sentencia Constitucional 0090/2014-S1» de fecha 24 de noviembre de 2014 [en línea]: https://buscador.tcpbolivia.bo/%28S%280hq5u0lzpaeb4xb4z1ubv3hd%29%29/WfrJurisprudencia.aspx [Consulta: 15/08/2015].

— (2015). *«Sentencia Constitucional 0189/2015-S3»* de fecha 10 de agosto de 2015 [en línea]: https://buscador.tcpbolivia.bo/%28S%280hq5u0lzpaeb4xb4z1ubv3hd%29%29/WfrJurisprudencia.aspx [Consulta: 18/09/2015].

— (2015). *«Sentencia Constitucional 0192/2015-S2»* de fecha 25 de febrero de 2013 [en línea]: https://buscador.tcpbolivia.bo/%28S%280hq5u0lzpaeb4xb4z1ubv3hd%29%29/WfrJurisprudencia.aspx [Consulta: 15/08/2015].

— (2015). *«Sentencia Constitucional 0332/2015-S1»* de fecha 6 de abril de 2015 [en línea]: https://buscador.tcpbolivia.bo/%28S%280hq5u0lzpaeb4xb4z1ubv3hd%29%29/WfrJurisprudencia.aspx [Consulta: 15/08/2015].

— (2015). *«Sentencia Constitucional 0426/2015-S3»* de fecha 20 de abril de 2015 [en línea]: https://buscador.tcpbolivia.bo/%28S%280hq5u0lzpaeb4xb4z1ubv3hd%29%29/WfrJurisprudencia.aspx [Consulta: 15/08/2015].

TRONCOSO R., A. (2006). *«La confidencialidad de la historia clínica»* en «Cuadernos de Derecho Público (27: enero-abril 2006). Instituto Nacional de Administración Pública.

VALDA D., J. J. (2014). *«Código Penal Boliviano Comentado: Concordancias, anotaciones doctrinales y jurisprudenciales, actualizado con las últimas reformas legislativas»*. Editorial e Imprenta El Original-San José, La Paz.

VALOR, J., y SÁEZ A., L. (2006). «Los sistemas de información» en «Gestión en el Sector de la Salud» Vol. 2. Elementos de gestión en las Instituciones. Pearson Educación, S. A. Madrid.

VÁZQUEZ I., C. (2002). *«Comercio electrónico, firma electrónica y servidores»*. DIJUSA Editorial, S. L., Madrid.

VILLABELLA A., C. M. (2009). «La investigación y la comunicación científica en la ciencia jurídica». Editado por el Instituto de Ciencias Jurídicas de Puebla. Departamento Editorial. México.

WIKIPEDIA (2008). *«Red privada virtual»* [en línea]: http://es.wikipedia.org/wiki/Red_privada_virtual [Consulta: 25/09/2008].

WINSIG (2015). *«Sistema de Información Gerencial de la OPS»* [en línea]: http://www.odontomarketing.com/art101ago2003.htm [Consulta: 11/01/2015].

ZIMIC, M., y otros (2009). *«Can the power of mobile phones be used to improve tuberculosis diagnosis in developing countries?»* Transactions of the Royal Society of Tropical Medicine and Hygiene, vol. 103, N.º 6 [en línea]: http://faculty.washington.edu/wcurioso/curioso_tbc_2008.pdf [Consulta: 26/06/2015].

ZUBIRI V., F. (2001). *«El secreto profesional médico. Normas y usos»*. Ediciones Mayo. Barcelona, p. 11-12, Cit. De Miguel S., N. (2002). «Secreto Médico, Confidencialidad e Información Sanitaria». Marcial Pons Ediciones Jurídicas y Sociales, S. A. Madrid.

ANEXOS

ANEXO 1 CONSENTIMIENTO INFORMADO

Estimado (a) paciente:

El consentimiento informado es la potestad que Usted tiene de aceptar libremente y sin presiones, que por necesidad diagnóstica o terapéutica, se practique en su propio cuerpo algún procedimiento clínico, laboratorial, imagenológico o instrumental, previa explicación clara de la persona que se lo practicará, con el fin de que usted sepa y comprenda cómo será realizado y cuáles son sus beneficios y eventuales riesgos o perjuicios, a más de obtener respuesta a sus preguntas e inquietudes.

En tal sentido, lea cuidadosamente este formulario y marque con una X la casilla que mejor se acomode a su respuesta.

1¿Acepta Usted voluntariamente ser internado en ……
……

SI ☐ NO ☐ ☐ Obligado por mi enfermedad

2.- ¿Desea Usted ser informado de todo lo que acontezca en el curso de su enfermedad?

SI ☐ NO ☐ ☐ Únicamente cuando yo pregunte

3.- ¿Da su consentimiento para someterse al interrogatorio y examen físico que permitan investigar las causas de su enfermedad y hacer el seguimiento de la misma?

SI ☐

SI ☐ Siempre y cuando sean realizados por personal autorizado y competente que se identifique con claridad, y proceda con el debido cuidado y respeto a mi pudor y privacidad.

NO ☐

4. ¿Acepta someterse a los exámenes clínicos de seguimiento cotidiano, así como a los controles y tratamientos rutinarios que ejerza el personal de enfermería?

SI ☐

SI ☐ Siempre y cuando sea informado sobre la naturaleza de los medicamentos que recibo y obedezcan a indicaciones precisas y escritas en mi Historia Clínica por los médicos tratantes de mi enfermedad.

NO ☐

5. ¿Acepta la colocación de sueros e inyectables sabiendo que el uso de agujas y catéteres puede provocarle alguna molestia o dolor, así como complicaciones locales (irritación, equimosis, abscesos localizados, hematomas) y complicaciones alérgicas de manifestación variable?

SI ☐

SI ☐ Siempre que en el lugar donde me encuentre tengan los recursos necesarios para resolver satisfactoriamente tales complicaciones.

NO ☐

6.- ¿Acepta la colocación de sondas o catéteres?

SI ☐

SI ☐ Siempre que de acuerdo a prescripción médica sean estrictamente necesarios

SI ☐ Siempre y cuando mi médico tratante me explique los efectos no deseados o complicaciones eventuales que pudieran provocar

NO ☐

7. - ¿Usted autoriza que le tomen muestras para exámenes de laboratorio por razones de su enfermedad?

SI ☐

SI ☐ Siempre y cuando sean estrictamente necesarios

SI ☐ Sin restricciones, siempre y cuando me sean explicadas las razones

NO ☐

8.- ¿Autoriza someterse a exámenes radiográficos y ecográficos que sus médicos tratantes consideren necesarios?

SI ☐

SI ☐ Siempre y cuando sean métodos simples, no invasivos y que no requieran introducción de medios de contraste en órganos cavitarios o en el torrente circulatorio

NO ☐

9.- ¿Dará Usted su consentimiento para someterse a procedimientos de diagnóstico o tratamiento más complejos que por razones de su enfermedad, pudieran ser necesarios?

SI ☐ Siempre y cuando la persona responsable de su realización me informe cabalmente sobre todas las implicaciones que tenga el procedimiento al que deba someterme.

SI ☐ Prefiriendo desconocer detalles ni ser informado sobre dichos procedimientos.

NO ☐

10.- ¿Acepta Usted la presencia de estudiantes o personas en formación cuando reciba la visita de su médico tratante o le sea practicado un examen clínico o cualquier otro procedimiento para el diagnóstico o tratamiento de su enfermedad?

SI ☐

SI ☐ Siempre que las personas sean pocas, me examine una sola y se respete mi pudor y privacidad

NO ☐

Firma, Nombre y Apellidos, números de registro de la persona que obtuvo el consentimiento

Firma o huella digital, nombre y apellidos, Cl de él o la paciente

Firma o huella digital, nombre y apellidos, Cl, del responsable o familiar

Lugar y fecha……..

FICHA ESPECÍFICA DE CONSENTIMIENTO INFORMADO

Para intervenciones quirúrgicas (médicas y de odontología)

Estimado paciente:

El consentimiento informado es la potestad que Usted tiene de aceptar libremente y sin presiones, que por necesidad diagnóstica o terapéutica, se practique en su propio cuerpo algún procedimiento clínico, laboratorial, imagenológico o instrumental, previa explicación clara de la persona que se lo practicará, con el fin de que usted sepa y comprenda cómo será realizado y cuáles son sus beneficios y eventuales riesgos o perjuicios, a más de obtener respuesta a sus preguntas e inquietudes.

Con este propósito, y para el caso en particular de la intervención quirúrgica que le será practicada, le solicitamos leer cuidadosamente este formulario, en cuya parte final encontrará Usted una casilla para marcar su aceptación o rechazo, seguida de su nombre completo y firma.

Nombre del paciente……..

Nombre del Establecimiento…….

Especificar si el paciente está internado o es ambulatorio ……..

…….....

Servicio o Unidad de Internación del paciente…….....

N° de Cama……N° de Expediente Clínico…….....

Nombre del cirujano principal que realizará la intervención quirúrgica…….....

…….....

Nombre técnico de la intervención quirúrgica…….....

Explicación literal y gráfica de la intervención quirúrgica

(Espacio libre para la descripción)

Duración aproximada de la intervención quirúrgica…….....

Medicamentos, substancias o materiales especiales que serán usados, administrados o colocados al paciente durante la realización de la intervención

quirúrgica……
……
……
.....
Utilidad (o necesidad) de la intervención quirúrgica…….....
……
.....
Beneficios de la intervención quirúrgica…….....
……
.....
Contraindicaciones de la intervención quirúrgica…….....
……
.....
Eventuales riesgos y peligros de la intervención quirúrgica…….....
……
……
……

La lectura de esta ficha ha sido acompañada de una explicación clara del cirujano principal encargado de realizar la intervención quirúrgica?

SI ☐ NO ☐

Una vez que Usted ha leído y llenado la presente ficha y habiendo comprendido cómo se realizará la intervención quirúrgica y cuáles son sus beneficios o eventuales perjuicios, sírvase señalar claramente si usted está de acuerdo o no con su realización.

Si estoy de acuerdo ☐ No estoy de acuerdo ☐

Nombre completo (paciente)
…….....
Firma o huella, y CI
…….....
Lugar y fecha
…….....

Nombre y Apellidos,
Sello, Nº registro y firma del profesional,
que hará la intervención quirúrgica

Nombre y Apellidos, firma o huella digital
C.I. del paciente o familiar responsable

ANEXO 2 GUÍA DE EVALUACIÓN DEL EXPEDIENTE CLÍNICO

Parámetros a Evaluar	INDICADORES	Cumplimiento		Observaciones y Conclusiones
		SI	NO	
Procedimientos establecidos para el proceso de atención	Registro de datos generales del paciente			
	Registro de Fecha de Ingreso			
	Registro del diagnóstico de Admisión			
Integridad y Claridad del Registro de la Historia Clínica	Historia Clínica abierta por el Médico de Guardia o de Sala, el mismo día de la admisión			
	La historia clínica contiene registro de anamnesis			
	Registro de motivo de consulta y enfermedad actual			
	Registro de tratamientos recibidos			
	Registro de exámenes realizados			
	Registro de evolución clínica			
	Registro de antecedentes patológicos y familiares			
	Registro de examen físico			
	Registro de examen neurológico			
	Registro de signos vitales			
	Registro de exámenes complementarios			
	Registro de diagnósticos diferenciales			
	Registro de diagnóstico de sala			
	Registro de tratamiento e indicación de exámenes complementarios			
Correlación entre el diagnóstico de admisión y el de sala	Justificación sobre la base del diagnóstico presuntivo de admisión para la internación			
	Relación entre el diagnóstico presuntivo de admisión y los diagnósticos diferenciales de sala			
Relación entre las indicaciones de tratamiento con el diagnóstico y protocolos de atención	Tratamiento en base a protocolos y fármacos del Listado Nacional de Medicamentos Esenciales			
Adecuación de la conducta terapéutica al manual de procedimientos	Relación entre la dosis, vía y tiempo de tratamiento con las normas de atención y evolución del paciente			
Justificación de los exámenes complementarios solicitados	Relación entre la solicitud de exámenes complementarios con los diagnósticos diferenciales o diagnósticos establecidos			
Correlación clínica epidemiológica del caso	Cumplimiento de criterios epidemiológicos para el control y seguimiento del caso según normas establecidas			
Evolución del paciente	Registro de evolución general			
	Registro de síntomas nuevos			
	Registro de respuesta al tratamiento			
	Registro de resultados de exámenes complementarios			
	Registro de cambios de medicación			
	Registro de Inter-consultas			
	Registro diario de órdenes médicas			
	Autorización del paciente para procedimientos médico-quirúrgicos			
Conducta Quirúrgica	Registro de justificación de la conducta quirúrgica			
	Registro de notas pre y post operatorias			
	Registro del protocolo quirúrgico			
	Registro notas de anestesiología			
	Registro de resultados de exámenes complementarios			
	Registro de complicaciones			
Días de internación	Relación entre el cuadro clínico y los días de internación			
Procedimientos del egreso Hospitalario	Registro de diagnósticos de ingreso			
	Registro de diagnósticos de egreso			
	Registro de fecha de ingreso			
	Registro de fecha de egreso			
	Registro de las causas del alta			
	Registro de los días de internación			
	Registro de defunción			
	Registro de conclusiones y datos de autopsia			

ANEXO 3 LEY Nº 3131 DEL EJERCICIO PROFESIONAL MEDICO

Art. 11 (Derechos del Médico)	Art. 12 (Deberes del Médico)
a) Una remuneración justa. b) Un trato digno del paciente, los familiares de éste y la comunidad. c) Trabajar en condiciones adecuadas para el desempeño de sus funciones. d) Ejercer la profesión en forma libre y sin presiones. e) Que se respete su criterio médico, diagnóstico y terapéutico y su libertad prescriptiva, así como su probable decisión de declinar la atención de algún paciente, siempre que tales aspectos se sustenten sobre bases éticas, científicas y protocolos vigentes. f) Recibir capacitación y actualización de su institución.	a) Cumplir con los principios éticos de la Declaración de Ginebra, aprobados por la Asociación Médica Mundial. b) Estar inscrito en el Colegio Médico de Bolivia. c) Colaborar a las autoridades del Sistema Nacional de Salud en caso de epidemias, desastres y emergencias. d) Respetar el consentimiento expreso del paciente, cuando rechace el tratamiento u hospitalización que se le hubiere indicado. e) Guiarse por protocolos oficiales cumpliendo con normas técnicas establecidas por el Ministerio del área de Salud. f) En caso de urgencia ningún médico, centro de salud, hospital o clínica podrá negar su atención básica. g) Brindar atención cuando una persona se encuentre en peligro inminente de muerte aún sin el consentimiento expreso. h) Otorgar los beneficios de la medicina a toda persona que los necesite, sin distinción alguna y sin más limitaciones que las señaladas por Ley. i) Informar al paciente, o responsables legales, con anterioridad a su intervención, sobre los riesgos que pueda implicar el acto médico. j) Cumplir con el llenado de los documentos médicos oficiales señalados en la presente Ley. k) Guardar el secreto médico, aunque haya cesado la prestación de sus servicios. l) Capacitación médica continua, para ello deberán someterse a los programas de capacitación y actualización periódica de conocimientos que definirá el Estado boliviano en forma obligatoria.
Art. 13 (Derechos del Paciente)	**Art. 14 (Deberes del Paciente)**
a) Recibir atención médica humanizada y de calidad. b) La dignidad como ser humano y el respeto a sus creencias y valores étnicos culturales. c) La confidencialidad. d) Secreto médico. e) Recibir información adecuada y oportuna para tomar decisiones libre y voluntariamente. f) Libre elección de su médico, de acuerdo a disponibilidad institucional. g) Reclamar y denunciar si considera que sus derechos humanos han sido vulnerados durante la atención médica. h) Disponer de un horario y tiempo suficiente para una adecuada atención. i) Respeto a su intimidad. j) Trato justo y equitativo sin desmedro de su condición socioeconómica, étnico cultural, de género y generacional. k) Solicitar la opinión de otro médico en cualquier momento. l) Negarse a participar en investigaciones o enseñanza de la medicina, salvo en situaciones que la Ley establece. m) m) Apoyar a la práctica médica como voluntarios en el tratamiento de enfermedades graves y ayudar a su rehabilitación.	a) Trato digno y respetuoso a su médico. b) Cumplir oportuna y disciplinadamente las prescripciones e indicaciones médicas. c) c) Comunicar de manera veraz y completa sus antecedentes de salud, personales y familiares.