AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

GUíA de Seguridad de Datos

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

NIPO: 052-08-003-6

Diseño Gráfico: ÉN

Imprime: NILO Industria Gráfica, S.A.

GUíA de Seguridad de Datos

GUíA

de Seguridad de Datos

indice

INTRODUCCIÓN

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD), establece en su punto 1 que "el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

El Reglamento de desarrollo de la LOPD (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre, fue publicado en el BOE número 17, de 19 de enero de 2008. El Título VIII de este reglamento desarrolla las medidas de seguridad en el tratamiento de datos de carácter personal y tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Entre estas medidas, se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

Con el objeto de facilitar a los responsables de ficheros y a los encargados de tratamientos de datos personales la adopción de las disposiciones del RLOPD, la Agencia Española de Protección de Datos pone a su disposición este documento, en el que se recopila un cuadro resumen de las medidas de seguridad recogidas en el citado Título VIII, un modelo de "Documento de Seguridad", que sirve de guía y facilita el desarrollo y cumplimiento de la normativa sobre protección de datos, y por último, una relación de comprobaciones con el objeto de facilitar la realización de la auditoría de seguridad.

AVISO IMPORTANTE:

Debe entenderse, en cualquier caso, que siempre habrá que atenerse a lo dispuesto en la LOPD, en el RLOPD, y en el resto de previsiones relativas a la protección de datos de carácter personal, y que la utilización de este modelo como guía de ayuda para desarrollar un "Documento de Seguridad" debe, en todo caso, tener en cuenta los aspectos y circunstancias aplicables en cada caso concreto, sin prejuzgar el criterio de la Agencia Española de Protección de Datos en el ejercicio de sus funciones.

En la web de la Agencia Española de Protección de Datos se encuentra disponible la versión actualizada de esta Guía de Seguridad (**www.agpd.es**)

MEDIDAS DE SEGURIDAD

Las medidas de seguridad exigibles a los ficheros y tratamientos de datos personales se clasifican en tres niveles: BÁSICO, MEDIO y ALTO.

APLICACION DE NIVELES

A continuación se indican los ficheros y tratamientos a los que corresponde aplicar las medidas de seguridad relativas a cada uno de los niveles que determina el RLOPD.

NIVEL ALTO. Ficheros o tratamientos con datos:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;
- recabados con fines policiales sin consentimiento de las personas afectadas; y
- derivados de actos de violencia de género.

NIVEL MEDIO. Ficheros o tratamientos con datos:

- relativos a la comisión de infracciones administrativas o penales;
- que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);
- de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;

- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;
- que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y
- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización [1]

NIVEL BÁSICO. Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
- se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero; y
- en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

MEDIDAS A APLICAR

EL DOCUMENTO DE SEGURIDAD

Es un documento interno de la organización, que debe mantenerse siempre actualizado. Disponer del documento de seguridad es una obligación para todos los responsables de ficheros y, en su caso, para los encargados del tratamiento, con independencia del nivel de seguridad que sea necesario aplicar.

Los apartados mínimos que debe incluir el documento de seguridad son los siguientes:

- ámbito de aplicación: especificación detallada de los recursos protegidos;
- medidas, normas, procedimientos, reglas y estándares de seguridad;
- funciones y obligaciones del personal,

1 Para esta categoría de ficheros además deberá disponerse de un registro de accesos

- estructura y descripción de los ficheros y sistemas de información;
- procedimiento de notificación, gestión y respuesta ante incidencias;
- procedimiento de copias de respaldo y recuperación de datos;
- medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.

A partir del nivel medio de medidas de seguridad, además de los apartados anteriores, deberán incluirse los siguientes:

- identificación del responsable de seguridad y
- control periódico del cumplimiento del documento

En caso de haber contratado la prestación de servicios por terceros para determinados ficheros, en el documento de seguridad se debe hacer constar esta circunstancia, indicando una referencia al contrato y su vigencia, así como los ficheros objeto de este tratamiento.

Si se ha contratado la prestación de servicios en relación con la totalidad de los ficheros y tratamientos de datos del responsable, y dichos servicios se prestan en las instalaciones del encargado del tratamiento se podrá delegar en éste la llevanza del documento de seguridad.

En el capítulo de "Guía modelo del Documento de seguridad" se encuentra el modelo que facilita la elaboración de este documento de seguridad.

	Nivel Básico	Nivel Medio	Nivel Alto
RESPONSABLE DE SEGURIDAD		El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.	
PERSONAL	Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. Definición de las funciones de control y las autorizaciones delegadas por el responsable. Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.		
INCIDENCIAS	Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. Procedimiento de notificación y gestión de las incidencias.	SOLO FICHEROS AUTOMATIZADOS Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. Autorización del responsable del fichero para la recuperación de datos.	
CONTROL DE ACCESO	Relación actualizada de usuarios y accesos autorizados. Control de accesos permitidos a cada usuario según las funciones asignadas. Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. Concesión de permisos de acceso sólo por personal autorizado. Mismas condiciones para personal ajeno con acceso a los recursos de datos.	SOLO FICHEROS AUTOMATIZADOS Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	SOLO FICHEROS AUTOMATIZADOS Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. Revisión mensual del registro por el responsable de seguridad. Conservación 2 años. No es necesario este registro si el responsable del fichero es una persona física y es el único usuario. SOLO FICHEROS NO AUTOMATIZADOS Control de accesos autorizados. Identificación accesos para documentos accesibles por múltiples usuarios.

	Nivel Básico	Nivel Medio	Nivel Alto
IDENTIFICACIÓN Y AUTENTICACIÓN	SOLO FICHEROS AUTOMATIZADOS Identificación y autenticación personalizada. Procedimiento de asignación y distribución de contraseñas. Almacenamiento ininteligible de las contraseñas. Periodicidad del cambio de contraseñas (<1 año).	SOLO FICHEROS AUTOMATIZADOS Limite de intentos reiterados de acceso no autorizado.	
GESTIÓN DE SOPORTES	Inventario de soportes. Identificación del tipo de información que contienen, o sistema de etiquetado. Acceso restringido al lugar de almacenamiento. Autorización de las salidas de soportes (incluidas a través de e-mail) Medidas para el transporte y el desecho de soportes.	SOLO FICHEROS AUTOMATIZADOS Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.	SOLO FICHEROS AUTOMATIZADOS Sistema de etiquetado confidencial. Cifrado de datos en la distribución de soportes. Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).
COPIAS DE RESPALDO	SOLO FICHEROS AUTOMATIZADOS Copia de respaldo semanal. Procedimientos de generación de copias de respaldo y recuperación de datos. Verificación semestral de los procedimientos. Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita. Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.		SOLO FICHEROS AUTOMATIZADOS Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
CRITERIOS DE ARCHIVO	SOLO FICHEROS NO AUTOMATIZADOS El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)		

	Nivel Básico	Nivel Medio	Nivel Alto
ALMACENAMIENTO	SOLO FICHEROS NO AUTOMATIZADOS Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.		SOLO FICHEROS NO AUTOMATIZADOS Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave.
CUSTODIA SOPORTES	SOLO FICHEROS NO AUTOMATIZADOS Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.		
COPIA O REPRODUCCIÓN			SOLO FICHEROS NO AUTOMATIZADOS Sólo puede realizarse por los usuarios autorizados. Destrucción de copias desechadas.
AUDITORIA		Al menos cada dos años, interna o externa. Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. Verificación y control de la adecuación de las medidas. Informe de detección de deficiencias y propuestas correctoras. Análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero.	
TELECOMUNICACIONES			SOLO FICHEROS AUTOMATIZADOS Transmisión de datos a través de redes electrónicas cifradas.
TRASLADO DOCUMENTACIÓN			SOLO FICHEROS NO AUTOMATIZADOS Medidas que impidan el acceso o manipulación.

- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.

- La ejecución de trabajos fuera de los locales del responsable o del encargado del tratamiento debe ser previamente autorizada por el responsable del fichero, constar en el documento de seguridad y garantizar el nivel de seguridad.

- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.

- Acceso facilitado a un encargado del tratamiento deberá constar en el documento de seguridad y deberá comprometerse al cumplimiento de las medidas de seguridad previstas.

ORGANIZACIÓN DEL MODELO

El RLOPD especifica que se puede disponer de un solo documento que incluya todos los ficheros y tratamientos con datos personales de los que una persona física o jurídica sea responsable, un documento por cada fichero o tratamiento, o los que determine el responsable atendiendo a los criterios organizativos que haya establecido. Cualquiera de las opciones puede ser válida. En este caso se ha optado por el primer tipo, organizando el "documento de seguridad" en dos partes: en la primera se recogen las medidas que afectan a todos los sistemas de información de forma común con independencia del sistema de tratamiento sobre el que se organizan: informatizado, manual o mixto, y en la segunda se incluye un anexo por cada fichero o tratamiento, con las medidas que le afecten de forma concreta. Además, se han especificado aquellas medidas que afectan sólo a ficheros automatizados y las que afectan a los no automatizados de forma exclusiva.

El modelo se ha redactado con el objeto de recopilar las exigencias mínimas establecidas por el Reglamento. Es posible y recomendable incorporar cualquier otra medida que se considere oportuna para aumentar la seguridad de los tratamientos, o incluso, adoptar las medidas exigidas para un nivel de seguridad superior al que por el tipo de información les correspondería, teniendo en cuenta la infraestructura y las circunstancias particulares de la organización.

Dentro del modelo se utilizarán los siguientes símbolos convencionales:
<comentario explicativo>: Entre los caracteres "<" y ">", se encuentran los comentarios aclaratorios sobre el contenido que debe tener un campo. Estos textos no deben figurar en el documento final, y deben desarrollarse para ser aplicados a cada caso concreto.

NIVEL MEDIO: con esta marca se señalarán las medidas que sólo son obligatorias en los ficheros que tengan que adoptar un nivel de seguridad medio.

NIVEL ALTO: Con esta marca se señalarán las medidas que sólo son obligatorias en los ficheros que tengan que adoptar un nivel de seguridad alto.

A: Con esta marca se señalarán las medidas específicas para aplicar exclusivamente a ficheros informatizados o automatizados.

M: Con esta marca se señalarán las medidas específicas para aplicar exclusivamente a ficheros manuales o no automatizados.

Las medidas que no van precedidas de ninguna de estas marcas deben aplicarse con carácter general, tanto a ficheros o tratamientos automatizados como no automatizados y con independencia del nivel de seguridad.

NOTA ACLARATORIA: Las medidas de seguridad de nivel básico son exigibles en todos los casos. Las medidas de nivel medio complementan a las anteriores en el caso de ficheros clasificados en este nivel, y las de nivel alto, cuando deban adoptarse, incluyen también las de nivel básico y medio.

DOCUMENTO DE SEGURIDAD

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el RLOPD recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la LOPD.

El contenido de este documento queda estructurado como sigue:

- Ámbito de aplicación del documento.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.

- Procedimiento general de información al personal.
- Funciones y obligaciones del personal.
- Procedimientos de notificación, gestión y respuestas ante las incidencias.
- Procedimientos de revisión.
- Consecuencias del incumplimiento del Documento de Seguridad.

ANEXO I. Descripción de ficheros.

ANEXO II. Nombramientos.

ANEXO III. Autorizaciones de salida o recuperación de datos.

ANEXO IV. Delegación de autorizaciones.

ANEXO V. Inventario de soportes.

ANEXO VI. Registro de incidencias.

ANEXO VII. Encargados de tratamiento.

ANEXO VIII. Registro de entrada y salida de soportes.

ANEXO IX. Medidas alternativas.

ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de <nombre del responsable>, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

NIVEL ALTO: Se aplicarán a los ficheros o tratamientos de datos:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;
- recabados con fines policiales sin consentimiento de las personas afectadas; y
- derivados de actos de violencia de género.

NIVEL MEDIO: Se aplicarán a los ficheros o tratamientos de datos:

- relativos a la comisión de infracciones administrativas o penales;
- que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);
- de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;
- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;
- que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y

- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización[2].

NIVEL BÁSICO: Se aplicarán a cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
- se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero; y
- en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

<incluir relación de ficheros o tratamientos afectados, indicando si se trata de sistemas automatizados, manuales o mixtos, y el nivel de seguridad que les corresponde>.
.....
.....
En el Anexo I se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

2 Para esta categoría de ficheros además deberá disponerse de un registro de accesos.

MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

IDENTIFICACIÓN Y AUTENTICACIÓN

Medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales.

A

- <Especificar las normativas de identificación y autenticación de los usuarios con acceso a los datos personales. La identificación de los usuarios se deberá realizar de forma inequívoca y personalizada, verificando su autorización (cada identificación debe pertenecer a un único usuario).

- Si la autenticación se realiza mediante contraseñas, detallar el procedimiento de asignación, distribución y almacenamiento que deberá garantizar su confidencialidad e integridad, e indicar la periodicidad con la que se deberán cambiar, en ningún caso superior a un año.

- También es conveniente incluir los requisitos que deben cumplir las cadenas utilizadas como contraseña>.

A

NIVEL MEDIO En los ficheros <indicar los nombres de los ficheros de nivel medio y alto>, se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

CONTROL DE ACCESO

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados <incluir estos mecanismos>.

Exclusivamente el <persona autorizada (o denominación de su puesto de trabajo) para conceder, alterar o anular el acceso autorizado> está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del fichero <nota: si la persona es diferente en función del fichero, incluir el párrafo en la parte del Anexo I correspondiente>.

<Especificar los procedimientos para solicitar el alta, modificación y baja de las autorizaciones de acceso a los datos, indicando qué persona (o puesto de trabajo) concreta tiene que realizar cada paso.

Incluir y detallar los controles de acceso a los sistemas de información>.

En el Anexo I, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista se actualizará <Especificar procedimiento de actualización>.

De existir personal ajeno al responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

NIVEL ALTO: REGISTRO DE ACCESOS

A

En los accesos a los datos de los ficheros de nivel alto, <indicar los nombres de los ficheros de nivel alto> se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido.

<Indicar si se estima oportuno, información relativa al sistema de registro de accesos. El mecanismo que permita este registro estará bajo control directo del responsable de seguridad, sin que se deba permitir, en ningún caso, la desactivación del mismo>.

Los datos del registro de accesos se conservaran durante <especificar periodo, que deberá ser al menos de dos años. No es preciso que estos datos se almacenen "on-line">.

El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe según se detalla en el capítulo de "Comprobaciones para la realización de la auditoría de seguridad" de este documento.

No será necesario el registro de accesos cuando:
- el responsable del fichero es una persona física,
- el responsable del fichero garantice que sólo él tiene acceso y trata los datos personales, y
- se haga constar en el documento de seguridad.

M

El acceso a la documentación se limita exclusivamente al personal autorizado.
Se establece el siguiente mecanismo para identificar los accesos realizados en el caso de los documentos relacionados <indicar los documentos o tipos de documentos que puedan ser utilizados por múltiples usuarios, así como el mecanismo establecido para controlar estos accesos; igualmente se definirá en este punto un registro de accesos general>.

GESTIÓN DE SOPORTES Y DOCUMENTOS

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en <indicar el lugar de acceso restringido donde se almacenarán>, lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación: <especificar el personal autorizado a acceder al lugar donde se almacenan los soportes que contengan datos de carácter personal, el procedimiento establecido para habilitar o retirar el permiso de acceso. Tener en cuenta el procedimiento a seguir para casos en que personal no autorizado tenga que tener acceso a los locales por razones de urgencia o fuerza mayor>.

Los siguientes soportes <relacionar aquellos a que se refiere> cumplirán con las obligaciones indicadas en el párrafo anterior, dadas sus características físicas, que imposibilitan el cumplimiento de las mismas.

Los siguientes soportes <indicar aquellos que contengan datos considerados especialmente sensibles y respecto de los que se haya optado por proceder del siguiente modo> se identificarán utilizando los sistemas de etiquetado siguientes <especificar los criterios de etiquetado que serán comprensibles y con significado para los usuarios autorizados, permitiéndoles identificar su contenido, y que sin embargo dificultarán la identificación para el resto de personas>.

Los soportes se almacenarán de acuerdo a las siguientes normas: <indicar normas de etiquetado de los soportes. Especificar el procedimiento de inventariado y almacenamiento de los mismos. El inventario de soportes puede anexarse al documento o gestionarse de forma automatizada, en este último caso se indicará en este punto el sistema informático utilizado>.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos, fuera de los locales bajo el control del responsable del tratamiento, deberá ser autorizada por el responsable del fichero o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento <detallar el procedimiento a

seguir para que se lleve a cabo la autorización. Tener en cuenta también los ordenadores portátiles y el resto de dispositivos móviles que puedan contener datos personales>.

En el Anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

Los soportes que vayan a ser desechados, deberán ser previamente <detallar procedimiento a realizar para su destrucción o borrado> de forma que no sea posible el acceso a la información contenida en ellos o su recuperación posterior.

En el traslado de la documentación se adoptarán las <indicar medidas y procedimientos previstos> para evitar la sustracción, pérdida o acceso indebido a la información.

A

NIVEL MEDIO : REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

Las salidas y entradas de soportes correspondientes a los ficheros <indicar los nombres de los ficheros de nivel medio y alto>, serán registradas de acuerdo al siguiente procedimiento: <Detallar el procedimiento por el que se registrarán las entradas y salidas de soportes>. El registro de entrada y salida de soportes se gestionará mediante <indicar la forma en que se almacenará el registro, que puede ser manual o informático> y en el que deberán constar <indicar los campos del registro, que deberán ser, al menos, en el caso de las entradas, el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la recepción; y en el caso de las salidas, el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la entrega>.

<En caso de gestión automatizada se indicará en este punto el sistema informático utilizado>.

A

NIVEL ALTO: GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

Los soportes relacionados <indicar aquellos de nivel alto> se identificarán mediante el sistema de etiquetado <especificar los criterios de etiquetado que resultarán comprensibles y con significado para los usuarios con acceso autorizados, permitiéndoles identificar su contenido y dificultando la identificación para el resto de personas>.

La distribución y salida de soportes que contengan datos de carácter personal de los ficheros <indicar los nombres de los ficheros de nivel alto> se realizará <indicar el procedimiento para cifrar los datos o, en su caso, para utilizar el mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte. Igualmente se cifrarán los datos que contengan los dispositivos portátiles cuando se encuentren fuera de las instalaciones que están bajo control del responsable>.

Los siguientes dispositivos portátiles <relacionar aquellos que no permitan el cifrado de los datos personales>, debido a las razones indicadas <motivar la necesidad de hacer uso de este tipo de dispositivos>, se utilizarán en el tratamiento de datos personales adoptándose las medidas que a continuación se explicitan <relacionar las medidas alternativas que tendrán en cuenta los riesgos de realizar tratamientos en entornos desprotegidos>.

M

CRITERIOS DE ARCHIVO

El archivo de los soportes o documentos se realizará de acuerdo con los criterios <indicar los previstos en la legislación que les afecte o en su defecto, los establecidos por el responsable del fichero, que en cualquier caso garantizarán la correcta conservación de los documentos, la localización y consulta de la información y posibilitarán el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación>.

M

ALMACENAMIENTO DE LA INFORMACIÓN

Los siguientes dispositivos <relacionarlos así como aquellas de sus características que obstaculicen su apertura. Cuando sus características físicas no permitan adoptar esta medida, el responsable adoptará medidas que impidan el acceso a la información de personas no autorizadas> se utilizarán para guardar los documentos con datos personales.

NIVEL ALTO: Los elementos de almacenamiento <indicar tipos como armarios, archivadores u otros elementos utilizados> respecto de los documentos con datos personales, se encuentran en <indicar lugares físicos y protección con que cuenta el acceso a las mismas, como llaves u otros dispositivos. Además estos lugares permanecerán cerrados en tanto no sea preciso el acceso a los documentos. Si a la vista de las características de los locales no fuera posible cumplir lo anteriormente indicado, se adoptarán medidas alternativas que se reflejarán en este punto>.

M

CUSTODIA DE SOPORTES

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamientos indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas.

ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

<Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones, sean o no públicas, garantizarán un nivel de seguridad equivalente al exigido para los accesos en modo local. Relacionar los accesos previstos y los ficheros a los que se prevea acceder>.

A

NIVEL ALTO: Los datos personales correspondientes a los ficheros <relacionar los de nivel alto>, que se transmitan a través de redes públicas o inalámbricas de comunicaciones electrónicas se realizará cifrando previamente estos datos <indicar en su caso otros mecanismos distintos del cifrado que se utilicen y que garanticen que la información no sea inteligible ni manipulada por terceros. También es adecuado cifrar los datos en red local>.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

Se pueden llevar a cabo los siguientes tratamientos de datos personales <relacionar los ficheros a que afecten estos tratamientos> fuera de los locales del responsable del fichero <indicar en su caso, los distintos locales a los que deban circunscribirse, especialmente en el supuesto de que se realicen tratamientos por un encargado del tratamiento que se especificará>, así como mediante dispositivos portátiles. Esta autorización regirá durante <indicar el período de validez de la misma>.

<Esta autorización puede realizarse para unos usuarios concretos que hay que indicar o para un perfil de usuarios>.

<Se debe garantizar el nivel de seguridad correspondiente>.

M

TRASLADO DE DOCUMENTACIÓN

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse las siguientes medidas <relacionar las medidas necesarias y en su caso alternativas recomendadas, orientadas a impedir el acceso o manipulación de la información objeto de traslado>.

FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

M

NIVEL ALTO

COPIA O REPRODUCCIÓN

La realización de copias o reproducción de los documentos con datos personales sólo se podrán realizar bajo el control del siguiente personal autorizado <indicar los usuarios o perfiles habilitados para ello>.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida <indicar los medios a utilizar o puestos a disposición de los usuarios para ello>.

A

COPIAS DE RESPALDO Y RECUPERACIÓN

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos, con la siguiente periodicidad <especificarla, y en todo caso será como mínimo una vez a la semana>.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente respecto de los ficheros parcialmente automatizados siguientes <indicarlos>, se grabarán manualmente los datos. <Para la grabación manual indicada deberá existir documentación que permita dicha reconstrucción>.

El responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

NIVEL ALTO: En los ficheros <indicar ficheros de nivel alto> se conservará una copia de respaldo y de los procedimientos de recuperación de los datos en <especificar el lugar, diferente de donde se encuentran los sistemas informáticos que los tratan, y que deberá cumplir las medidas de seguridad, o utilizando elementos que garanticen la integridad y recuperación de la información de forma que sea recuperable>.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD

Se designa como responsable de seguridad <indicarlo/s en el caso de que se prevea que sean varios>, que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad. <La designación puede ser única para todos los ficheros o diferenciada según los sistemas de tratamiento, lo que se especificará en este documento, en la parte correspondiente del Anexo I>.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde a <denominación responsable del fichero o del encargado del tratamiento> como responsable del fichero de acuerdo con el RLOPD.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de <indicar periodo de desempeño del cargo>. Una vez transcurrido este plazo <denominación responsable del fichero> podrá nombrar al mismo responsable de seguridad o a otro diferente.

En el Anexo II se encuentran las copias de los nombramientos de responsables de seguridad.

PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el Capítulo siguiente y de forma específica para cada fichero en la parte del Anexo I correspondiente.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento: <indicar el procedimiento por el cual se informará a cada persona, en función de su perfil, de las normas que debe cumplir y de las consecuencias de no hacerlo. Puede ser conveniente incluir algún sistema de acuse de recibo de la información>.

<Si se estima oportuna, la remisión periódica de información sobre seguridad: circulares, recordatorios, nuevas normas, indicar aquí el procedimiento y las personas autorizadas para hacerlo>.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

FUNCIONES Y OBLIGACIONES DE CARÁCTER GENERAL.

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al <responsable del fichero o de seguridad en su caso> las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias".

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Funciones y obligaciones de <incluir un punto con las obligaciones detalladas de los perfiles que afectan a todos los ficheros, como por ejemplo, administradores de los sistemas, responsables de informática, responsable/s de seguridad si existe/n, responsables de seguridad física, etc. Es importante que se concrete la persona o cargo que corresponde a cada perfil. También deben contemplarse los procedimientos de actuación o delegación de funciones para casos de ausencia. Este apartado se propone principalmente como un recopilatorio que agrupe las medidas que en el resto del Documento se asignan a perfiles concretos>.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto de aquellos datos que hubiera podido conocer durante la prestación del servicio.

Se delegan las siguientes autorizaciones en los usuarios relacionados <indicar usuarios, o perfiles y autorizaciones que el responsable del fichero delega en ellos para su ejercicio>.

PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de <denominación del responsable del fichero>.

El procedimiento a seguir para la notificación de incidencias será <especificar concretamente los procedimientos de notificación y gestión de incidencias, indicando quien tiene que notificar la incidencia, a quien y de que modo, así como quien gestionará la incidencia>.

El registro de incidencias se gestionará mediante <indicar la forma en que se almacenará el registro, que puede ser manual o informático, y en el que deberán constar, al menos, el tipo de incidencia, el momento en que se ha producido o en su caso detectado, la persona que realiza la notificación, a quién se comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. En caso de gestión automatizada se indicará en este punto el sistema informático utilizado>.

A

NIVEL MEDIO: En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros <relacionar los ficheros de nivel medio y alto>, del modo que se indica a continuación <detallar el procedimiento para registrar las recuperaciones de datos, que deberá incluir la persona que ejecutó el proceso, los datos restaurados y, en su caso, que datos ha sido necesario grabar manualmente en el proceso de recuperación. En caso de gestión automatizada, se deberá prever la existencia de un código específico para recuperaciones de datos, en la información relativa al tipo de incidencia>.

NIVEL MEDIO: Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del responsable del fichero.

En el Anexo III se incluirán los documentos de autorización del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

PROCEDIMIENTOS DE REVISIÓN

REVISIÓN DEL DOCUMENTO DE SEGURIDAD

<Especificar los procedimientos previstos para la modificación del documento de seguridad, con especificación concreta de las personas que pueden o deben proponerlos y aprobarlos, así como para la comunicación de las modificaciones al personal que pueda verse afectado.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal>.

NIVEL MEDIO: AUDITORÍA

<Indicar los procedimientos para realizar la auditoría interna o externa que verifique el cumplimiento del Título VIII del RLOPD, referente a las medidas de seguridad, según lo indicado en sus artículos 96 y 110 respecto de ficheros automatizados y no automatizados respectivamente, y que debe realizarse al menos cada dos años.

Con carácter extraordinario deberá realizarse cuando se lleven a cabo 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 auditoria inicia el cómputo de dos años señalado.

El informe analizará la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

Los informes de auditoría han de ser analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos, o en su caso de las autoridades de control de las comunidades autónomas>.

NIVEL ALTO: INFORME MENSUAL SOBRE EL REGISTRO DE ACCESOS

<Indicar los procedimientos para realizar el informe mensual sobre el registro de accesos a los datos de nivel alto regulado por el artículo 24 del RLOPD>.

CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a <indicar la normativa sancionadora aplicable>.

ANEXO I
DESCRIPCIÓN DE FICHEROS

Actualizado a: <fecha de la última actualización del anexo>.

<Se incluirá un anexo de este tipo por cada fichero incluido en el ámbito del documento de seguridad, podrían denominarse ANEXO I a, b, c, etc.>.

- Nombre del fichero o tratamiento: <rellenar con nombre del fichero>.
- Unidad/es con acceso al fichero o tratamiento: <especificar departamento o unidad con acceso al fichero, si aporta alguna información>.
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos: <rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)>.
    - □ Identificador: <código de inscripción>.
    - □ Nombre: <nombre inscrito>.
    - □ Descripción: <descripción inscrita>.
- Nivel de medidas de seguridad a adoptar: <básico, medio o alto>.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD

<Persona designada por el responsable del fichero al objeto de coordinar y controlar las medidas incluidas en este documento para este fichero, en el caso de que existan varios, o para todos los ficheros en el supuesto de que se trate de designación única>.

- Administrador: <persona designada para conceder, alterar, o anular el acceso autorizado a los datos>.

- Leyes o regulaciones aplicables que afectan al fichero o tratamiento <si existen>.

- Código Tipo Aplicable: <se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el articulo 32 de la LOPD>.

- Estructura del fichero principal: <incluir los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 81 del Reglamento de desarrollo de la LOPD >.

- Información sobre el fichero o tratamiento

  - □ Finalidad y usos previstos.
  - □ Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales, y procedencia de los datos: <indicar proce dencia de los datos, quién suministra los datos>.
  - □ Procedimiento de recogida: <encuestas, formularios en papel, Internet, ...>.
  - □ Cesiones previstas: <relacionar los destinatarios de los datos previstos>.
  - □ Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>.
  - □ Sistema de tratamiento: <automatizado, manual o mixto>.

- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: <indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>

- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.

- Información sobre conexión con otros sistemas: <Describir las posibles relaciones con otros ficheros del mismo responsable>.

- Funciones del personal con acceso a los datos personales: <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.

- Descripción de los procedimientos de control de acceso e identificación: <Cuando sean específicos para el fichero>.

- Relación actualizada de usuarios con acceso autorizado: <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.

<Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.

ANEXO II
NOMBRAMIENTOS

<Adjuntar original o copia de los nombramientos que afecten a los diferentes perfiles incluidos en este documento, como el del responsable de seguridad>.

ANEXO III
AUTORIZACIONES DE SALIDA O RECUPERACIÓN DE DATOS

<Adjuntar original o copia de las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, así como aquellas relativas a la ejecución de los procedimientos de recuperación de datos>.

ANEXO IV
DELEGACIÓN DE AUTORIZACIONES

En su caso, personas en las que el responsable del fichero ha delegado <Indicar las autorizaciones, tales como: salida de dispositivos portátiles, la copia o reproducción de documentos en soporte papel, …>.

ANEXO V
INVENTARIO DE SOPORTES

<Si el inventario de soportes se gestiona de forma no automatizada recoger en este anexo la información al efecto, según lo indicado en el apartado de "Gestión de soportes y Documentos" de este documento. Los soportes deberán permitir identificar el tipo de información, que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en este documento>.

ANEXO VI
REGISTRO DE INCIDENCIAS

<Si el registro de incidencias se gestiona de forma no automatizada, recoger en este anexo la información al efecto, según lo indicado en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias" de este documento>.

ANEXO VII
ENCARGADOS DE TRATAMIENTO

<Cuando el acceso de un tercero a los datos del responsable del fichero sea necesario para la prestación de un servicio a este último, no se considera que exista comunicación de datos. Recoger aquí el contrato que deberá constar por escrito o de alguna otra forma que permita acreditar su celebración y contenido, y que establecerá expresamente que el encargado de tratamiento tratará los datos conforme a las instrucciones del responsable del tra-

tamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, y que no los comunicarán, ni siquiera para su conservación a otras personas.

El contrato estipulará las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento esta obligado a implementar>.

ANEXO VIII
REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

<Si el registro de entrada y salida de soportes al que se refiere el apartado de "Gestión de soportes y Documentos", y que es obligatorio a partir del nivel medio, se gestiona de forma no automatizada, recoger en este anexo la información al efecto, según lo indicado el artículo 97 del RLOPD>.

ANEXO IX
MEDIDAS ALTERNATIVAS

<En el caso de que no sea posible adoptar las medidas exigidas por el RLOPD en relación con la identificación de los soportes, los dispositivos de almacenamiento de los documentos o los sistemas de almacenamiento de la información, indicar las causas que justifican que ello no sea posible y las medias alternativas que se han adoptado>.

COMPROBACIONES PARA LA REALIZACIÓN DE LA AUDITORÍA DE SEGURIDAD

OBJETIVO

Determinar si se han establecido, si son adecuadas y si se cumplen las medidas de seguridad recogidas en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Su realización es obligatoria para ficheros de nivel medio y alto. Puede ser interna o externa. Debe realizarse al menos cada dos años. Excepcionalmente, si se han realizado modificaciones sustanciales en el sistema de información, deberá realizarse una auditoría para comprobar la adecuación, adaptación y eficacia de las medidas de seguridad. Esta auditoría iniciará el cómputo de dos años.

DETERMINACIÓN DEL ALCANCE DE LA AUDITORÍA

Se debe establecer cuáles son los ficheros con datos de carácter personal objeto de la auditoría, tratamientos sobre los mismos, sistemas de tratamiento, procedimientos, etc.

PLANIFICACIÓN

Determinar los recursos necesarios para llevar a cabo la auditoría, las fuentes de información, la ubicación del fichero o las instalaciones, etc.

RECOLECCIÓN DE DATOS

- Relación de ficheros, estructura y contenido.
- Políticas de seguridad y procedimientos (registro de incidencias, copias de respaldo y recuperación, Identificación y autorización, borrado de soportes, cifrado, etc.).
- Documento de Seguridad y auditorías anteriores (si las hubiese).
- Diseño físico y lógico de los sistemas de información.
- Relación de usuarios, accesos autorizados y sus funciones.
- Inventario de soportes y registro de entrada y salida de soportes.
- Registros de acceso e informes de revisión de los mismos.
- Entrevistas a usuarios, técnicos de sistemas, responsables, etc.
- Inspección visual.
- etc.

EVALUACIÓN DE LAS PRUEBAS

Se relacionan a continuación algunas comprobaciones que se pueden realizar para verificar el cumplimiento de las disposiciones del Reglamento:

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
ASPECTOS GENERALES		
TODOS	¿La clasificación del nivel de seguridad es adecuada respecto a la naturaleza de la información contenida en cada uno de los ficheros y su finalidad?	BÁSICO
	¿Se han creado, modificado o suprimido ficheros con datos de carácter personal desde la última auditoría?	
ENCARGADO DE TRATAMIENTO		
TODOS	¿Se realiza el tratamiento por persona distinta al responsable del fichero?, ¿se ha formalizado mediante contrato conforme lo establecido el artículo 12 de la LOPD?	BÁSICO
	Si la realización de este encargo se realiza en los locales del responsable ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?, ¿consta por escrito en el contrato el compromiso del personal del encargado de tratamiento respecto al cumplimiento de las medidas de seguridad recogidas en el Documento de Seguridad del responsable?	
	Cuando el tratamiento se realiza mediante acceso remoto a los sistemas del responsable ¿se le ha prohibido al encargado de tratamiento la incorporación de los datos a sistemas o soportes distintos de los del responsable?, ¿se ha hecho constar tal circunstancia en el Documento de Seguridad del responsable?	
	Si la prestación se hace en locales propios del encargado de tratamiento (distintos de los del responsable) ¿ha elaborado el encargado el documento de seguridad?, ¿identifica el fichero o tratamiento y el responsable del mismo?, ¿detalla las medidas de seguridad a implementar en relación con su tratamiento?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
PRESTACIÓN DE SERVICIO SIN ACCESO A DATOS PERSONALES		
TODOS	Si el tratamiento no afecta a datos personales ¿se han adoptado las medidas necesarias para limitar el acceso del personal a los datos personales, soportes y recursos?	BÁSICO
	Si se trata de personal ajeno ¿recoge el contrato la prohibición expresa de acceder a los datos personales, así como la obligación de secreto respecto a los datos que hubieran podido conocer con motivo de la prestación de servicio?	
DELEGACIÓN DE AUTORIZACIONES		
TODOS	¿Se han delegado las autorizaciones que el Reglamento atribuye al responsable en otras personas?, ¿se ha hecho constar en el Documento de Seguridad las personas habilitadas para otorgar estas autorizaciones y las personas en quienes recae dicha delegación?	BÁSICO
RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO		
TODOS	El almacenamiento de datos personales en dispositivos portátiles o los tratamientos fuera de los locales del responsable o del encargado ¿han sido autorizados expresamente por el responsable del fichero?, ¿consta dicha autorización en el Documento de Seguridad?	BÁSICO
	¿Se garantiza el nivel de seguridad correspondiente al tipo de fichero tratado?	
FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS		
TODOS	¿Cumplen el nivel de seguridad correspondiente?	BÁSICO
	¿Se han destruido o borrado cuando ya no han sido necesarios para los fines que motivaron su creación?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	DOCUMENTO DE SEGURIDAD	
TODOS	¿Ha elaborado el responsable del fichero el Documento de Seguridad?	BÁSICO
	¿Contiene los aspectos mínimos exigidos por el Reglamento?	
	¿Está el documento actualizado?, ¿se ha revisado cuando se han producido cambios relevantes desde la auditoría anterior?	
	¿Está su contenido adecuado a la normativa vigente en este momento en materia de seguridad de los datos de carácter personal?	
	¿Se ha indicado con qué periodicidad se deben cambiar las contraseñas?, ¿es inferior o igual a un año?	
	¿Se especifica cuál es el personal autorizado para la concesión, alteración o anulación de accesos autorizados sobre datos o recursos?	
	¿Se especifica cuál es el personal autorizado para acceder a los lugares donde se almacenan los soportes informáticos?	
	Si el tratamiento se realiza por cuenta de terceros ¿se han reflejado los ficheros afectados por el encargo, con referencia expresa al contrato, así como la identificación del responsable y el periodo de vigencia?	
	¿Se ha reflejado en el Documento de Seguridad si los datos personales se incorporan y tratan exclusivamente en los sistemas del encargado?	
	¿Se ha delegado en el encargado del tratamiento la llevanza del Documento de Seguridad para los ficheros objeto del contrato?, ¿se ha reflejado esta circunstancia en el contrato?	
	¿Establece la identidad del responsable o responsables de seguridad?, ¿se especifica si la designación es única para todos los ficheros o está diferenciada según el sistema de tratamiento utilizado?	MEDIO
	¿Contiene los procedimientos y controles periódicos a realizar para verificar el cumplimento de lo dispuesto en el propio documento?	
	¿Especifica qué medidas hay que adoptar en caso de desechado o reutilización de soportes?	
	¿Relaciona las personas que están autorizadas a acceder físicamente a los locales donde se ubican los sistemas de información?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
FUNCIONES Y OBLIGACIONES DEL PERSONAL		
TODOS	Están las funciones y obligaciones del personal con acceso a datos de carácter personal y los sistemas de información claramente definidos?	BÁSICO
	¿Están documentadas y reflejadas en el documento de seguridad?	
	¿Se han definido las funciones de control o autorizaciones delegadas por el responsable del fichero?	
	¿Conoce el personal las medidas de seguridad que afectan al desarrollo de sus funciones?	
	¿Conoce las consecuencias de su incumplimiento?	
REGISTRO DE INCIDENCIAS		
TODOS	¿Existe un procedimiento de notificación y gestión de incidencias de seguridad?, ¿el procedimiento está bien diseñado y es eficaz? ¿Conoce todo el personal afectado dicho procedimiento?	BÁSICO
	¿Existe un registro de incidencias donde se reflejen todos los datos exigidos en el Reglamento?, ¿se han registrado todas las incidencias ocurridas?	
	¿Se revisa periódicamente el registro de incidencias para su análisis y adopción de medidas correctoras de las incidencias anotadas?	
AUTOMATIZADO	¿Se han anotado las ejecuciones de los procedimientos de recuperación de datos realizados?	
	¿Figuran en estas anotaciones los datos exigidos por el Reglamento?	MEDIO
	¿Existe la autorización por escrito del responsable del fichero?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	CONTROL DE ACCESO	
TODOS	¿Los accesos autorizados de los usuarios se corresponden exclusivamente a los datos y recursos que precisan para el desarrollo de sus funciones?	BÁSICO
	¿Existen mecanismos que impidan que los usuarios accedan a datos o recursos distintos de los autorizados?	
	¿Existe una relación de usuarios?, ¿especifica qué datos y recursos tiene autorizados para cada uno de ellos? ¿Está actualizada?	
	¿La concesión, alteración o anulación de accesos autorizados sobre datos y recursos la realiza exclusivamente el personal autorizado para ello en el Documento de Seguridad?	
	¿Ha establecido el responsable del fichero los criterios conforme a los cuales se otorga la autorización de los accesos a los datos y a los recursos?	
	El personal ajeno al responsable que tiene acceso a los datos y recursos de éste ¿se encuentra sometido a las mismas condiciones y obligaciones que el personal propio?	
AUTOMATIZADO	¿El acceso a los locales donde se encuentran ubicados los sistemas de información se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?	MEDIO
NO AUTOMATIZADO	¿Se encuentran los archivadores u otros elementos de almacenamiento en áreas de acceso restringido dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente?, ¿están cerradas estas áreas mientras no sea preciso el acceso a los documentos incluidos en el fichero?	ALTO
	Si los locales del responsable no permiten disponer de un área de acceso restringido ¿ha adoptado el responsable medidas alternativas?, ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?, ¿se ha motivado adecuadamente?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	GESTION DE SOPORTES Y DOCUMENTOS	
TODOS	¿Está identificado el tipo de información contenido en el soporte o documento?	BÁSICO
	¿Existe y se mantiene un inventario de soportes?	
	¿Se almacenan los soportes o documentos en lugares de acceso restringido?	
	¿Existen mecanismos por los que solamente puedan acceder las personas autorizadas en el Documento de Seguridad?, ¿funcionan adecuadamente estos mecanismos?	
	¿Se ha dejado constancia en el Documento de Seguridad, si fuera el caso, de la imposibilidad de cumplir con las obligaciones establecidas en el Reglamento sobre identificación, inventariado y acceso a los soportes dadas sus características físicas?	
	¿La salida de soportes y documentos fuera de los locales donde se ubica el fichero está siendo autorizada por el responsable del fichero o está debidamente autorizada en el Documento de Seguridad?	
	¿Se están tomando las medidas adecuadas en el traslado de documentación para evitar la sustracción, perdida o acceso indebido durante su transporte?	
	Cuando se desecha un soporte o documento conteniendo datos de carácter personal ¿se adoptan las medidas adecuadas para evitar el acceso a la información o su recuperación posterior cuando se procede a su destrucción o borrado?, ¿son adecuadas estas medidas?	
	¿Se dan de baja en el inventario estos soportes o documentos desechados?	
	Para los soportes con datos de carácter personal considerados especialmente sensibles por la organización ¿se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto?, ¿son adecuados y cumplen su finalidad?	
	¿Existe un registro de entrada de soportes o documentos?, ¿y un registro de salida?	MEDIO
	¿Contienen estos registros de entrada y salida de soportes toda la información exigida en el Reglamento?	
	¿Las personas encargadas de la recepción y la entrega de soportes están debidamente autorizadas?, ¿Consta en el Documento de Seguridad dicha autorización?	
	¿Se han anotado todas las entradas y salidas de soportes?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	GESTION DE SOPORTES Y DOCUMENTOS (CONT.)	
AUTOMATIZADO	¿Se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto? ¿son adecuados y cumplen su finalidad?	ALTO
	¿La distribución de soportes se realiza de forma cifrada, o por otro mecanismo que garantice que no sea inteligible o manipulable durante el transporte?	
	¿Se cifran los datos en los dispositivos portátiles cuando éstos salen de las instalaciones del responsable del fichero?	
	Si fuera imprescindible el tratamiento de datos en dispositivos portátiles que no permitan el cifrado de datos ¿se ha hecho constar motivadamente en el Documento de Seguridad?, ¿se han adoptado medidas para minimizar los riesgos derivados de este tratamiento en entornos desprotegidos?, ¿son adecuadas?	
NO AUTOMATIZADO	¿Se adoptan medidas que impidan el acceso o manipulación de la información en los casos de traslado físico de la documentación contenida en un fichero?, ¿son apropiadas estas medidas?	
	La generación de copias o reproducción de documentos ¿se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?	
	¿Se destruyen las copias o reproducciones desechadas de forma que no se pueda acceder a la información contenida en las mismas?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	IDENTIFICACIÓN Y AUTENTICACIÓN	
AUTOMATIZADO	¿Existe una relación de usuarios con acceso autorizado?, ¿se mantiene actualizada?	BÁSICO
	¿Existen procedimientos de identificación y autenticación para dicho acceso?, ¿garantiza la correcta identificación del usuario?	
	El mecanismo de acceso y verificación de autorización de los usuarios ¿les identifica de forma inequívoca y personalizada?	
	¿Existe un procedimiento de asignación, distribución y almacenamiento de contraseñas?, ¿garantiza su confidencialidad e integridad?	
	¿Se cambian las contraseñas con la periodicidad establecida en el documento de seguridad?	
	¿Se almacenan las contraseñas de forma ininteligible mientras están en vigor?	
	¿Se limita el intento reiterado de acceso no autorizado al sistema?, ¿se anotan estos intentos en el registro de incidencias?	MEDIO

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	COPIAS DE RESPALDO Y RECUPERACIÓN	
AUTOMATIZADO	¿El responsable del fichero ha definido los procedimientos de realización de copias de respaldo y recuperación de los datos?, ¿es adecuada esta definición?	BÁSICO
	¿Están reflejados estos procedimientos en el Documento de Seguridad?	
	¿Ha verificado el responsable del fichero la correcta aplicación de estos procedimientos?, ¿realiza esta verificación cada seis meses?	
	¿Garantizan los procedimientos establecidos la reconstrucción de los datos al estado en que se encontraban antes de producirse la pérdida o destrucción?	
	Si esta pérdida o destrucción afecta a ficheros parcialmente automatizados ¿se ha procedido a grabar manualmente los datos?, ¿queda constancia motivada de este hecho en el Documento de Seguridad?	
	¿Se realizan copias de respaldo al menos semanalmente? Si no es así ¿se debe a que no ha habido actualizaciones en ese periodo?	
	¿Las pruebas previas a la implantación o modificación de los sistemas de información se realizan con datos reales? En caso afirmativo, ¿se están aplicando las mismas medidas de seguridad que las que le corresponde por la naturaleza de los datos que contiene?, ¿se anota su realización en el Documento de Seguridad?, ¿se hacen copias de seguridad previas a la realización de pruebas con datos reales?	
	¿Se conserva una copia de respaldo y de los procedimientos de recuperación de datos en lugar diferente al de los equipos que los tratan?	ALTO
	¿Cumple este lugar las medidas de seguridad exigidas en el Reglamento?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
REGISTRO DE ACCESOS		
AUTOMATIZADO	¿Existe el registro de accesos? En caso negativo ¿concurren en el responsable alguna de las circunstancias que le eximen de este requisito? ¿se ha hecho constar en el Documento de Seguridad?	ALTO
	¿Se está recogiendo en este registro la información mínima exigida en el Reglamento?	
	¿Los mecanismos que permiten el registro de estos accesos están directamente bajo el control del responsable de seguridad?	
	¿Existe la posibilidad de desactivar estos mecanismos?	
	¿Se conservan los datos registrados por un período mínimo de dos años?	
	¿Revisa el responsable de seguridad periódicamente la información registrada?	
	¿Realiza el responsable de seguridad un informe, al menos mensualmente, con el resultado de las revisiones realizadas y los problemas detectados?	
NO AUTOMATIZADO	¿El acceso a la documentación se realiza exclusivamente por personal autorizado?	
	¿Existen mecanismos para identificar los accesos realizados cuando los documentos son utilizados por múltiples usuarios?	
	¿Se ha establecido un procedimiento para registrar el acceso de personas no incluidas en el caso anterior?, ¿es adecuado?	
ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES		
AUTOMATIZADO	¿Los accesos a datos mediante redes de comunicaciones garantizan un nivel de seguridad equivalente a los accesos en modo local?	BÁSICO
AUTOMATIZADO	¿La transmisión de datos a través de redes se realiza de forma cifrada (o por cualquier otro mecanismos que garantice que la información no sea inteligible ni manipulada por terceros)?, ¿este mecanismo de cifrado es eficaz?	ALTO

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	AUDITORÍA	
TODOS	¿Se realiza la actual auditoría en el plazo establecido desde la anterior?	MEDIO
	Si ha habido modificaciones sustanciales en el sistema de información ¿se ha realizado a continuación una auditoría para verificar la adaptación, adecuación y eficacia de las medidas de seguridad?	
	¿Los informes de las auditorías anteriores incluían los datos, hechos y observaciones en los que se basaban sus dictámenes?	
	¿Se han implementado las medidas correctoras propuestas por auditorías anteriores?, ¿han sido eficaces y han corregido las deficiencias encontradas?	
	CRITERIOS DE ARCHIVO	
TODOS	¿Existe legislación específica con criterios para el archivo de soportes o documentos?, ¿garantizan estos criterios la conservación de documentos, la localización y consulta de la información?, ¿posibilitan el ejercicio de los derechos de oposición, acceso, rectificación y cancelación?	BÁSICO
	En caso de no existir legislación específica ¿ha establecido el responsable del fichero los criterios y procedimientos de actuación para el archivo de documentos?, ¿es adecuado este procedimiento?	
	ALMACENAMIENTO DE LA INFORMACIÓN	
NO AUTOMATIZADO	¿Los dispositivos de almacenamiento de documentos disponen de mecanismos que obstaculicen su apertura? Si sus características físicas no permiten adoptar esta medida ¿ha adoptado el responsable medidas que impidan el acceso de personas no autorizadas?	BÁSICO
	CUSTODIA DE SOPORTES	
NO AUTOMATIZADO	¿Se custodia correctamente la documentación cuando ésta no se encuentra archivada en los dispositivos de almacenamiento por estar en revisión o tramitación?, ¿se impide en todo momento que sea accedida por persona no autorizada?	BÁSICO

ELABORACIÓN DEL INFORME

- Debe dictaminar sobre:
- Adecuación de las medidas y controles establecidas a lo dispuesto en el Título VIII del Reglamento.
- Identificación de deficiencias y propuesta de medidas correctoras o complementarias.
- Incluirá los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.
- Será analizado por el responsable de seguridad, y elevará sus conclusiones al responsable del fichero para que adopte las medidas adecuadas.
- Deberá quedar a disposición de la Agencia Española de Protección de Datos.

PREGUNTAS FRECUENTES

NIVELES DE SEGURIDAD

¿Cuándo se aplica el nivel básico de seguridad a datos de salud?

El artículo 81.6 del Reglamento de desarrollo de la LOPD señala que "podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos."

Por tanto dos son los factores que deben concurrir necesariamente para aplicar medidas de nivel básico en este caso: 1) la existencia de una ley que imponga un deber cuyo cumplimiento obligue a tratar ciertos datos de salud; y 2) que dichos datos respondan a unas características concretas.

En el primer caso, y a título de ejemplo, pueden citarse las obligaciones contempladas en la legislación sobre IRPF o Seguridad social, que en los ficheros de nóminas obligan a tratar datos como el porcentaje de discapacidad o la existencia de una incapacidad laboral.

En el segundo caso, se podrá aplicar el nivel básico, tratándose de datos de salud, únicamente, en los siguientes tipos de dato:

DISCAPACIDAD	porcentaje, indicador "SI/NO"
Incapacidad laboral, enfermedad común, accidente laboral, enfermedad profesional	"SI/NO" fecha
Aptitud para el desempeño (por razones de salud)	"Apto/no apto".
Maternidad	"SI/NO"

La regulación del artículo. 81.6 RDLOPD establece una excepción y por tanto debe ser interpretada restrictivamente. Por tanto, si no se trata de esta tipología de datos personales no podrá aplicarse. De ahí que en el caso de que se incluya referencia a un dato específico de salud, como por ejemplo, la enfermedad concreta relacionada con el motivo de la baja laboral o un código que la identifique, el nivel aplicable será el ALTO.

Además debe existir una ley que imponga la obligación de tratar el dato y por ello, si en un fichero se incluye voluntariamente un dato del tipo "porcentaje de discapacidad" sin que exista obligación legal el nivel aplicable al fichero será ALTO.

Por último, la presencia aislada de alguno de estos datos no prejuzga necesariamente el nivel de seguridad aplicable. Así por ejemplo, la presencia de un dato del tipo apto/no apto en un fichero dedicado a la prevención de riesgos que incluya el historial clínico-laboral del trabajador no permite aplicar el nivel básico ya que, habida cuenta del contenido de la citada historia clínica procederá aplicar el nivel de seguridad ALTO.

- **¿Cuándo podrá aplicarse el nivel básico de medidas de seguridad a un fichero que contenga datos especialmente protegidos como la afiliación sindical?**

El artículo 81.5.a) permite aplicar el nivel básico en caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

Existen dos ejemplos en los que se aprecia con claridad el criterio para aplicar esta excepción. En primer lugar, en el caso de que se tenga previsto tratar el dato relativo a las cuotas sindicales se deberá tener en cuenta que la deducción de la cuota sindical es una obligación impuesta por Ley al empresario. Así, el artículo 11 de la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical, establece que:

- *En los convenios colectivos podrán establecerse cláusulas por las que los trabajadores incluidos en su ámbito de aplicación atiendan económicamente la gestión de los sindicatos representados de la comisión negociadora, fijando un canon económico y regulando las modalidades de su abono. En todo caso, se respetará la voluntad individual del trabajador, que deberá expresarse por escrito en la forma y plazos que se determinen en la negociación colectiva.*

- *El empresario procederá al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de éste*".

Si atendemos al precepto anterior resulta claro que se impone al empresario un deber que se traduce en practicar un descuento y transferirlo al sindicato, es evidente que los datos relativos a la afiliación sindical son datos especialmente protegidos conforme al artículo 7 LOPD. No obstante, la excepción del Reglamento permite adoptar las medidas de seguridad de nivel básico.

Del mismo modo, y en segundo lugar, idéntica situación se produce en el caso de domiciliaciones bancarias para el pago de cuotas a sindicatos, partidos, confesiones, asociaciones etc. en los que la que el banco o caja trata los datos con la única finalidad de realizar la gestión consistente en un pago.

¿Qué se entiende por ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan datos especialmente protegidos?

En relación con el nivel de medidas de seguridad aplicable, sería necesario atender al tenor literal del artículo 81.5 del RLOPD que establece que "En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

- Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad."

A este respecto, se debería tener en cuenta que la excepción prevista en el último inciso del artículo 81.5 se refiere a cuando los datos especialmente protegidos sean incluidos por el propio afectado a la hora al presentar documentación en la que por propia iniciativa desee aportar este tipo de datos, sin que su tratamiento tenga relación con la finalidad establecida por el responsable del fichero.

Es fundamental tener en cuenta que esta excepción únicamente se aplicara a los ficheros no automatizados.

¿Qué nivel de seguridad debe adoptarse en los ficheros que contengan datos de menores?

En esta materia el RLOPDen su artículo 13, únicamente regula la forma de recabar el consentimiento de los menores, sin que ello afecte, en modo alguno, a las medidas de seguridad que deben de adaptarse a los ficheros o tratamientos de datos por parte del responsable.

La regulación de las medidas de seguridad, se encuentran en el Título VIII, Capítulo I artículos del 79 al 86. Así el artículo 80 señala que "Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto." Por otra parte el artículo 81 regula la aplicación estos niveles de seguridad.

Por lo tanto, la determinación del nivel de seguridad que debe de adoptar un responsable dependerá de los criterios fijados por el artículo 81 del Reglamento para el que la condición de la minoría de edad no es relevante.

ENCARGADOS Y PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS

¿Qué obligaciones en materia de medidas de seguridad tienen los encargados de tratamiento?

Tanto las prestaciones de servicios realizadas por los encargados de tratamiento en los locales del responsable del fichero, como las realizadas en los propios locales del encargado, se encuentran sujetas a la normativa de protección de datos.

Con carácter general, las obligaciones del encargado del tratamiento en materia de implantación de las medidas de seguridad se encuentran reguladas en los artículos 82 y 88 del Reglamento de desarrollo de la LOPD. Además el documento de seguridad de un encargado debe tener un contenido adicional específico que permita identificar sus encargos indicando:

- La identificación de los ficheros o tratamientos que se traten en concepto de encargado.
- Referencia expresa al contrato o documento que regule las condiciones del encargo.
- Identificación del responsable.
- Período de vigencia del encargo.

En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a los restantes requisitos establecidos en el Reglamento de la LOPD.

Por último, el encargado de tratamiento debe implantar las medidas de seguridad adecuadas para sus propios ficheros. Entre ellas, debe mantener actualizado su documento de seguridad, fijar las obligaciones de su personal etc.

¿Puede el encargado hacerse cargo del documento de seguridad del responsable que le ha contratado?

No es infrecuente la existencia de tratamientos, como por ejemplo la confección de nóminas, en los que los datos se alojan y tratan casi por completo en los locales, recursos y soportes del encargado. Para estos casos, el reglamento se refiere en su artículo 88 a la "delegación de la llevanza del documento de seguridad". Para ello deben cumplirse ciertos requisitos:

- Que los datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado.
- Que esta circunstancia afecte a parte o a la totalidad de los ficheros o tratamientos del responsable.
- Que la delegación se indique de modo expreso en el contrato celebrado al amparo del artículo 12 LOPD, con especificación de los ficheros o tratamientos afectados.

No podrá delegarse en el encargado la llevanza del documento de seguridad en lo relativo a aquellos datos contenidos en recursos propios del responsable.

En las prestaciones sin acceso a datos ¿qué obligaciones de seguridad existen?

Se deberá tener en cuenta que la mayoría de las actividades que supongan un contacto directo o indirecto con el sistema de información y/o con su entorno físico o lógico puede ser susceptible de poner en riesgo la seguridad de los datos.

Así por ejemplo, el servicio de seguridad que custodia las llaves de las instalaciones debe ser advertido de las políticas de control de acceso físico a las instalaciones y de las eventuales restricciones de acceso que se hayan fijado.

Del mismo modo, los servicios de limpieza deberían ser informados de aspectos relacionados con las prohibiciones relacionadas con el desechado de documentos, -por ejemplo, utilizar medios convencionales como el contenedor de basuras-, o de la necesidad de que en determinadas salas se mantengan condiciones de refrigeración que garanticen la estabilidad de las máquinas que soportan el sistema de información.

Un último ejemplo, lo proporcionan los servicios de mantenimiento que, eventualmente, deben tener obligaciones cuando sus acciones pueden poner en peligro un sistema, - por ejemplo, la de advertir cuando una reparación haga necesario desconectar la red eléctrica obligando a un copiado y/o apagado preventivo.

En estos casos, para la realización de trabajos que no impliquen el tratamiento de datos personales, y de conformidad con lo establecido en el artículo 83 del Reglamento de la LOPD, el responsable del fichero debe adoptar las medidas adecuadas para limitar el acceso del personal a los datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios deberá recoger expresamente la prohibición de acceder a los datos personales y la obligación de secreto que el personal debe observar.

DOCUMENTO DE SEGURIDAD

□ ¿Qué debo hacer para documentar y/o notificar las funciones y obligaciones del personal?

La descripción de las funciones del personal con acceso a datos de carácter personal tienen que estar incluidas en el documento de seguridad y formarán parte de las medidas organizativas que el responsable del fichero y, en su caso, el encargado del tratamiento debe implantar.

El procedimiento de documentación y transmisión de las políticas que incluyan las funciones y obligaciones del personal con acceso a datos de carácter personal, puede ser diverso dependiendo de las particularidades de cada organización, pudiendo utilizarse documentos escritos, comunicaciones electrónicas, ya sea mediante correo electrónico, intranet corporativa, páginas de inicio de las aplicaciones, etc.

En todo caso, será necesario que el responsable del fichero y, en su caso, el encargado del tratamiento se aseguren que el personal con acceso a datos de carácter personal conoce las funciones y obligaciones que tiene con respecto al acceso a los datos de carácter personal, en particular, en lo relativo al deber de secreto y confidencialidad.

□ ¿Qué permite la delegación de autorizaciones?

La delegación de autorizaciones, a la que se refiere el artículo 84 del Reglamento, es una posibilidad que permite flexibilizar la gestión de la seguridad en materia de protección de datos de carácter personal.

Esta previsión habilita al responsable para delegar en otras personas las funciones que el Reglamento atribuye al responsable del fichero. Estas delegaciones deben estar recogidas en el documento de seguridad y no suponen, en ningún caso, trasladar a la persona en quien se delega la responsabilidad en la que pudiera incurrir la organización o persona responsable del fichero.

□ ¿Debe contener el registro de incidencias detalle de los problemas asociados a aspectos puramente técnicos de los ficheros: averías, caídas de tensión, problemas de red o conectividad?

El objetivo fundamental de implantar las medidas de seguridad a las que se refiere la LOPD (art. 9) y su Reglamento de desarrollo es garantizar que los datos de carácter personal se tratan con las adecuadas garantías que permitan asegurar la confidencialidad, la integridad y la disponibilidad de los datos.

En éste ámbito las incidencias poseen una gran relevancia debido tanto a su propia capacidad para comprometer los objetivos de la seguridad como por el conocimiento que su resolución aporta a los responsables. Así, por ejemplo una avería eléctrica puede poner en peligro la disponibilidad de un sistema de información.

Teniendo en cuenta los objetivos de la seguridad, la inclusión de las incidencias de este tipo deberá realizarse siempre cuando con motivo del funcionamiento de estos servicios la seguridad pudiera verse comprometida.

□ ¿Cuál es el alcance y el objetivo del registro de incidencias?

La obligación de establecer un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal, así como establecer un registro en el que se hagan constar los detalles de dichas incidencias, se encuentra regulado en el artículo 90 y 100 del Reglamento, dependiendo que el nivel de medidas de seguridad requeridas sea básico o medio.

El objetivo final perseguido por el Reglamento a este respecto, tal y como lo señala en el artículo 90 citado, es que se adopten las medidas correctoras para que dicha incidencia sea controlada, por lo que debe mantenerse una acción permanente de control, revisión y actuación sobre las medidas implantadas y las incidencias detectadas.

□ ¿Cuál es el alcance de la obligación de anotar las salidas de soportes mediante correo electrónico?

El envío de ficheros con datos de carácter personal mediante correo electrónico o fax conlleva ciertos riesgos específicos que deberán ser analizados por el responsable del fichero y, en su caso, por el encargado del tratamiento para establecer las medidas técnicas y organizativas que deben implantarse para controlar los riesgos inherentes a la utilización del dichos medios, en función de los tipos de datos que vayan ser objeto de transmisión.

En cualquier caso, tal y como establece el artículo 92 del Reglamento la salida de soportes y documentos que contengan datos de carácter personal, como los incluidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento, deberá ser autorizada por el responsable o ser debidamente autorizada en el documento de seguridad.

En el caso de los ficheros que deben implantar las medidas catalogadas como de nivel medio, el artículo 97 del Reglamento establece la obligación de disponer de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer la información relacionada con el envío. En el caso de las medidas de seguridad de nivel alto, la distribución de los soportes deberá realizarse cifrando los datos o utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte (art. 101 Reglamento).

Por lo que respecta concretamente al sistema de registro, en el caso de que se remitan datos de carácter personal incluidos en un anexo a un correo electrónico, el propio gestor del correo electrónico puede servir como registro.

Esta obligación de anotar las salidas afecta a cualquier otro procedimiento electrónico como el protocolo FTP, descargas desde Internet, carpetas compartidas, así como al envío de fax cuando incorporan datos de carácter personal de un fichero o tratamiento.

- **¿Debe registrarse la salida de soportes con destino a otra sede de la entidad? ¿Y a la del encargado?**

Deben anotarse tanto en uno como en el otro caso, ya que se trata de asegurar el control y la trazabilidad de los soportes con datos de carácter personal que salen materialmente del sistema de información del responsable del fichero.

¿Debe notificarse a la AEPD el documento de seguridad?

El documento de seguridad es un documento interno de la organización y no debe ser notificado a la Agencia Española de Protección de Datos, quedando a disposición de la Agencia o, en su caso, de las autoridades de protección de datos de las Comunidades Autónomas.

MEDIDAS CONCRETAS

¿Qué significa guardar las copias de respaldo en lugar físico diferente?

Para los ficheros con datos de carácter personal sujetos a la obligación de implantar las medidas de nivel alto, el reglamento de desarrollo de la LOPD prevé la obligación de conservar una copia de respaldo de los datos de estos ficheros y de los procedimientos de recuperación de los mismos en un lugar diferente del que se encuentran los equipos informáticos que los tratan (art. 102 Reglamento LOPD), con el fin de que no se encuentren sometidos a las mismas contingencias que pudiera sufrir el lugar habitual de almacenamiento en caso de un accidente o desastre, como por ejemplo, un incendio o una inundación.

En el caso de que no sea posible guardar una copia de los ficheros en un lugar distinto y no sujeto a los mismos riesgos, se deberán adoptar medidas complementarias para paliar el riesgo, tales como ubicar la copia en armarios ignífugos, implantación de sistemas antiincendio, etc). En estos casos, cuando la sede del responsable cuente con distintas estancias o niveles de edificación se entenderá por lugar distinto una estancia diferenciada del lugar principal en el que se ubiquen los sistemas de información, preferiblemente en planta distinta y más protegida y, se deberá hacer constar estas circunstancias en el documento de seguridad.

Debe hacerse notar que la obligación de realizar copias de respaldo no es aplicable a los ficheros no automatizados, con independencia del resto de medidas aplicables e este tipo de ficheros, entre las que deberán observarse las previsiones establecidas en el Reglamento

de la LOPD, entre otras, en lo relativo a la custodia de los soportes y dispositivos de almacenamiento, así como a la copia o reproducción de los documentos con datos de carácter personal.

- **¿Cuál es el ámbito de la auditoría establecida en el RLOPD? ¿Quién debe realizarla? ¿Debe notificarse?**

El ámbito de la auditoría, previsto en el artículo 96 para los ficheros automatizados y 110 para los no automatizados, se refiere a la verificación del cumplimiento de las medidas de seguridad que deben implantarse en los ficheros automatizados y no automatizados con datos de carácter personal establecidas en el Título VIII del Reglamento de desarrollo de la LOPD, sin perjuicio de que cuando alguna de las materias reguladas la LOPD se proyecten sobre las medidas de seguridad deban ser tenidas en cuenta.

Así por ejemplo, es evidente que una salida de datos podría tener relación con una comunicación de datos pudiendo analizarse su licitud. Del mismo modo, la existencia de un encargado del tratamiento puede comportar una evaluación conexa del contenido del contrato.

Sobre quién debe realizarla, el Reglamento establece que puede ser interna o externa y no define el perfil funcional o profesional de los auditores, aunque la propia función de auditoría ha de llevar implícita la independencia y la debida capacitación profesional para que resulte adecuada para la función de verificación que pretende llevar a cabo.

Por último, el informe de auditoría deberá ser analizado por el responsable de seguridad que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de la comunidades autónomas, no siendo necesario su notificación a la AEPD.

¿Cuál debe ser el alcance del registro de accesos?

La obligación de implantar y guardar, durante un período mínimo de dos años, los datos relativos a los accesos realizados a los datos catalogados como de nivel alto, prevista en el artículo 103 del Reglamento de la LOPD, persigue que se pueda identificar el registro accedido. En este sentido, el objetivo es el de ser capaz de establecer las acciones realizadas por un determinado usuario respecto del registro accedido sin necesidad de que tal conocimiento alcance al contenido concreto de la información accedida.

El citado artículo establece la información mínima que deberá guardarse de cara acceso a los datos de carácter personal sujetos a la obligación de implantar las medidas de nivel alto.

Así mismo, se establecen las circunstancias concretas en las que el Reglamento excepciona de la obligación de implantar el registro de accesos: el responsable debe ser una persona física y debe ser el único usuario del sistema. Esta circunstancia deberá hacerse constar en el documento de seguridad.

¿Cómo aplico el control de acceso previsto para los ficheros no automatizados o manuales?

En el caso de los ficheros no automatizados con nivel alto de seguridad, el Reglamento de la LOPD establece, en su artículo 113 las medidas que han de adoptarse para controlar el acceso a la documentación a la que deba implantarse las medidas de nivel alto.

Para implantar este control de acceso a la documentación se podrán utilizar, por ejemplo:

- Plantillas básicas en soporte papel incorporadas al inicio del expediente.
- Registros automatizados en la gestión de entradas y salidas al archivo.
- Cualquier otro sistema o procedimiento que permita alcanzar la finalidad perseguida por el Reglamento.

OTROS ASPECTOS

En caso de una sanción por falta de medidas de seguridad ¿qué responsabilidad tiene el Responsable de Seguridad?

La responsabilidad de implantar las medidas de seguridad en los ficheros con datos de carácter personal recae en el responsable del fichero y, en su caso, en el encargado del tratamiento.

Así, entre las medidas organizativas se procederá a nombrar uno o varios responsables de seguridad. Esta designación es una previsión establecida en el Reglamento de la LOPD para los ficheros que tengan que implantar las medidas de seguridad catalogadas como de nivel medio y alto.

La medida que establece el artículo 95 del Reglamento, no puede suponer, en ningún caso, una exoneración de la responsabilidad que corresponda al responsable del fichero o al encargado del tratamiento.

- **¿Qué tengo que pedir al proveedor cuando adquiera un producto software que trate datos de carácter personal?**

La Disposición adicional única del Reglamento de desarrollo de la LOPD establece que los productos software destinados al tratamiento automatizado de datos de carácter personal deberán incluir en su descripción técnica el nivel de seguridad que tiene implantado, por lo que cuando se adquiera o se contrate la construcción de un aplicativo software que trate datos de carácter personal, se deberá pedir que el constructor especifique el nivel de medidas de seguridad que cumple el producto.

- **Para el cómputo de plazos para la implantación de las medidas de seguridad ¿cuándo se considera que son ficheros preexistentes?**

Se consideran ficheros preexistentes a los efectos de, en su caso, disponer del período transitorio para implantar las medidas de seguridad al que se refiere la Disposición transitoria segunda del Reglamento de desarrollo de la LOPD, los ficheros que hubieran sido notificados para su inscripción con anterioridad a la entrada en vigor del Reglamento de desarrollo de la LOPD, aprobado mediante el RD 1720/2007, de 21 de diciembre, publicado en el BOE del 19 de enero de 2008.

FICHEROS EXISTENTES		NIVEL	PLAZO
AUTOMATIZADOS	SEGURIDAD SOCIAL, MUTUAS, PERFILES	MEDIO	1 AÑO
	VIOLENCIA DE GÉNERO	MEDIO	1 AÑO
		ALTO	18 MESES
	TELECOMUNICACIONES (TRÁFICO, LOCALIZACIÓN) REGISTRO DE ACCESOS	MEDIO	1 AÑO 18 MESES
	ADAPTACIÓN RESTO DE FICHEROS		1 AÑO
NO AUTOMATIZADOS		BÁSICO	1 AÑO
		MEDIO	18 MESES
		ALTO	2 AÑOS

Dado que en la citada disposición se establecía la entrada en vigor del Reglamento a los tres meses de su publicación en el BOE, tendrán la consideración de ficheros preexistentes, a los efectos de la implantación de las medidas de seguridad, los ficheros que hayan sido notificados al Registro General de Protección de Datos hasta el día 19 de abril de 2008.

Cualquier fichero notificado con posterioridad deberá incorporar el conjunto de medidas previstas para el nivel de seguridad que le corresponda.

En la web de la Agencia Española de Protección de Datos, se encuentra disponible la versión actualizada de las preguntas frecuentes relacionadas con esta Guía de Seguridad.

www.agpd.es

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

www.agpd.es