

PLANES SECTORIALES DE OFICIO SOBRE LAS TRANSFERENCIAS INTERNACIONALES. ACTUACIONES DE LA INSPECCION DE DATOS

José López Calvo
Subdirector General de Inspección de Datos

18 – Julio - 2007

1. OBJETIVO

Verificar el efectivo cumplimiento de la Ley Orgánica 15/1999 y su normativa de desarrollo en los centros de atención telefónica a clientes establecidos por empresas del sector de las telecomunicaciones.

2. PREMISAS

- La habilitación jurídica. El contrato escrito habilita a la AEPD para auditar al importador en la misma medida que lo haría respecto del exportador de datos conforme a la legislación española.**
- La existencia de precedentes en el ámbito internacional en otros sectores.**
- La colaboración de las empresas.**

3. REPRESENTATIVIDAD DEL SECTOR Y EMPRESAS

En mayo de 2007 para todo el sector de telecomunicaciones, constaban un total de 22 autorizaciones de transferencias internacionales de datos, que representan un 15% del total de autorizaciones.

La inspección de datos ha centrado las actuaciones de investigación en las transferencias autorizadas a dos operadores del sector de las telecomunicaciones que ofrecen la explotación del servicio de atención telefónica comercial, el servicio de atención de averías y telemarketing, en relación con los servicios de telefonía fija, telefonía móvil al sector de autónomos y pequeña y mediana empresa. Gestión de backoffice.

4. FASES

Metodología empleada en tres fases.

- **Primera fase:** visitas presenciales a las sedes de los operadores de telecomunicaciones, para concretar los servicios prestados desde Colombia.
- **Segunda fase:** inspecciones a las entidades encargadas de tratamiento que dispongan de sede en España.
 - . Evaluar el entorno tecnológico utilizado para la transferencia. Líneas de comunicación.
 - . Estudiar medidas de seguridad (no acceso a Internet, no transferencia ficheros, acceso a España, no sistema periférico).
 - . Comprobar que la información a la que se accede es adecuada.

- **Tercera fase.** Visitas a los encargados de los tratamientos ubicados en Colombia. Se han detectado dos casuísticas distintas.

En el caso de entidades españolas con **sucursal en Colombia**, la visita se planteó como una inspección realizada en un local de la entidad que actúa como encargado del tratamiento.

Visita presencial a los encargados de tratamiento **con sede únicamente en Colombia**. En este caso no se había realizado comprobación en España al no tener sede como encargado de tratamiento.

5. Servicios realizados que requieren tratamiento de datos

- Explotación del servicio de atención telefónica comercial al cliente residencial. Llamadas de clientes y tratamiento de datos relacionados con provisiones pendientes y facturación.
- Atención telefónica a clientes autónomos y pequeña y mediana empresa.
- Telemarketing a clientes.

6. Entorno tecnológico. Comunicación

Línea propietaria:

En el caso de empresa española prestadora de servicios con sucursal en Colombia se utilizan dos enlaces de fibra óptica que conectan directamente una sede de la entidad ubicada en España. Esto permite que los usuarios que trabajan desde Colombia tengan acceso a los mismos servicios y recursos que los que lo hacen desde la red de área local de los centros españoles.

Línea compartida (dedicada):

Respecto a la entidad prestadora de servicios con sede únicamente en Colombia, la estructura tecnológica de deslocalización se basa en el alquiler de líneas, propiedad del operador con quién han contratado la prestación de servicio origen de la transferencia internacional.

TRATAMIENTOS DE DATOS AUDITADOS

Los tratamientos de datos corresponden con los servicios especificados en los contratos aportados en la solicitud de las transferencias internacionales.

Los datos personales que tienen acceso las entidades encargadas del tratamiento se consideran los necesarios para la prestación de los servicios contratados.

El acceso a los datos personales se efectúa directamente sobre los Sistemas de Información y ficheros de los responsables ubicados en territorio nacional e independientemente de la ubicación geográfica del encargado del tratamiento.

MEDIDAS DE SEGURIDAD

Medidas adoptadas por los responsables de los ficheros:

Los operadores de telecomunicaciones han adoptado diversas medidas, entre otras, no permitir la realización de réplicas de los ficheros con datos personales fuera del territorio español, utilizar líneas dedicadas de comunicaciones para los accesos desde Colombia y haber implementado dispositivos de seguridad lógica.

La confidencialidad en los accesos a la información se realiza estableciendo un canal cifrado entre extremos.

Los accesos realizados por teleoperadores ubicados tanto en España como en Colombia quedan reflejados en los Sistemas de Información de los operadores de telecomunicación auditados.

Han anulado en todos los puestos de trabajo utilizados por los teleoperadores los dispositivos periféricos que permiten extraer información.

La identificación y autenticación de los teleoperadores ubicados en Colombia, se realiza mediante la utilización de un código de usuario y una contraseña a través de una herramienta propiedad del responsable del fichero que gestiona la asignación de las contraseñas y los perfiles de acceso a los datos.

8. Recomendaciones

PRIMERA: En relación con la Seguridad de los Datos Personales.

- En los casos que permiten obtener una evaluación de la personalidad del ciudadano, debe garantizarse la adopción de las medidas de seguridad de nivel medio en lo concerniente a la obligatoriedad de la realización de una auditoria bienal sobre el cumplimiento del Reglamento de Seguridad, establecimiento de un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al Sistema de Información y a la verificación de que está autorizado, a los controles de acceso físicos adecuados, así como al establecimiento de un registro de entrada y salida de soportes con datos de carácter personal.

b) Acceso a través de redes.

El acceso a los datos de carácter personal a través de redes de telecomunicaciones, debe realizarse con las medidas de seguridad que garanticen un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

c) Identificación y Autenticación.

Procedimiento de asignación, distribución y almacenamiento de contraseñas.

- Los usuarios que accedan a datos de carácter personal deberán poderse identificar de forma inequívoca y personalizada.**
- Perfiles de acceso.**
- Sistema de gestión integral de códigos de usuarios y contraseñas.**

d) Funciones y obligaciones del 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 deben estar claramente definidas.

e) Registro de incidencias

f) Auditorias

El Reglamento de Medidas de Seguridad obliga a la realización de una auditoria de seguridad interna o externa que verifique el cumplimiento de dicho Reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años, a partir del nivel medio. Cuando no sea legalmente exigible, se considera una buena práctica su implantación en las transferencias internacionales analizadas.

g) Terminales de acceso a los datos

Se recomienda que en los puestos de trabajo deslocalizados se anulen todos aquellos dispositivos periféricos.

SEGUNDA: En relación con el acceso a los datos por cuenta de terceros.

Las empresas inspeccionadas, el exportador y el importador han de suscribir un contrato de prestación de servicios, a tenor de lo dispuesto en el art. 12 de la LOPD.

Deberá indicarse que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento.

TERCERA: En relación con el deber de secreto. Medidas oportunas para que los trabajadores estén informados.