Boletín 02/11

LOPD EN LA EMPRESA

comSeveral
TIEMPO COSTE CALIDAD

LA LOPD EN EL DÍA A DÍA

¿Qué autorizaciones deben estar documentadas?

El cumplimiento del RD1720/2007 requiere que tengamos en el Documento de Seguridad las personas y/o perfiles a las que se ha concedido alguna de estas autorizaciones:

- Lista de usuarios que pueden sacar datos personales fuera de las instalaciones del responsable del fichero (N. Básico).
- Lista de usuarios que pueden tratar datos personales fuera de las instalaciones del responsable (N. Básico).
- Lista de usuarios que pueden tratar datos personales en dispositivos portátiles fuera de las instalaciones del responsable (N. Básico).
- Lista de usuarios que tienen acceso a los dispositivos (armarios, cajoneras, etc.) donde se almacenan los soportes que contienen datos personales (N. Básico).
- Lista de usuarios que tienen acceso a los locales donde están los sistemas de información (equipos) que tratan los ficheros (N. Medio).
- Lista de usuarios autorizados para enviar y/o recepcionar soportes automatizados que contienen datos personales (N. Medio).
- Lista de usuarios autorizados para copiar documentos que contienen datos personales de nivel alto (N. Alto).

Contenido

IMPORTANTE

Estas listas de usuarios autorizados deben mantenerse en todo momento actualizadas, reflejando la realidad de la organización.

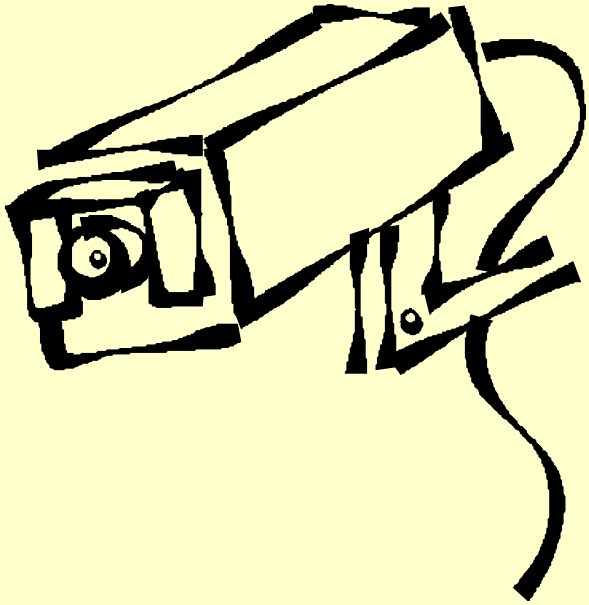
SANCIONES DE LA AEPD

Denuncia de la policía municipal a la AEPD

En el procedimiento sancionador PS/00327/2010 de la AEPD podemos ver cómo la propia **POLICIA MUNICIPAL DE MADRID denuncia la instalación** de un sistema de videovigilancia que no cumple los requisitos de la LOPD.

Las instalaciones de videovigilancia son las que más denuncias provocan ante la AEPD.

Según los hechos, la policía municipal de Madrid denuncia ante la Agencia Española de Protección de Datos la instalación de cámaras de videovigilancia en el establecimiento "La Cervesía", titularidad de BBT-LO VALERO, S.L. sin cumplir los requisitos exigidos por la LOPD.



Los inspectores de la AEPD constatan que en dicho establecimiento **no existen los carteles informativos de videovigilancia** donde se informa a los afectados de la existencia de dicho tratamiento, así como de la identidad del responsable del mismo y dónde pueden ejercer sus derechos.

En este caso la entidad denunciada ha **recabado datos personales sin facilitar a sus titulares la información** que señala el artículo 5 de la LOPD por lo que debe considerarse que ha incurrido en la infracción leve descrita (**multa de 601,01 a 60.101,21 €**).

Teniendo en cuenta los criterios de graduación de las sanciones previstos en el citado artículo 45.4 de la LOPD y, en especial, la falta de beneficios obtenidos y al grado de intencionalidad, la AEPD procede a **sancionar** al establecimiento "La Cervesía" con una **multa de 2.000€.**

IMPORTANTE

Como hemos visto en este caso, la denunciante es la propia **policía municipal**, que ha puesto el caso en manos de la AEPD **actuando "de oficio"** al detectar que una instalación de **videovigilancia** no estaba de acuerdo a la LOPD.

No ha sido necesaria la denuncia de ninguna persona que se haya sentido vulnerada al grabarla sin informarla previamente.

LA AEPD ACLARA

Conservación del informe de auditoría

El informe 0191/2010 de la AEPD aclara el plazo de conservación de los informes de auditoría que exige la LOPD para los ficheros de nivel medio y alto.

De dicho informe jurídico se extrae lo siguiente:

- **A partir de nivel medio** los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos **cada dos años, a una auditoria** interna o externa.

- Con **carácter extraordinario** deberá realizarse dicha auditoria siempre que se **realicen modificaciones sustanciales** en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. **Esta auditoria inicia el cómputo de dos años** señalado en el párrafo anterior.

- Teniendo en cuenta los plazos de prescripción y de **obligación** de sometimiento a la auditoría, el término durante el cual el **informe debería estar a disposición** de la Agencia Española de Protección de Datos o autoridad autonómica de control competente debería ser el de **dos años**.

A TENER EN CUENTA

Debe encontrarse a disposición de la Agencia Española de Protección de Datos el último informe de auditoría, emitido, no siendo preciso mantener a su disposición los anteriores a aquel.

ACTUALIDAD LOPD

La AEPD publica una guía práctica para ciudadanos sobre "sus derechos a la protección de datos"

Fuente: *www.agpd.es*

Puede descargarse este guía desde:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf

EL PROFESIONAL RESPONDE

¿Qué sistemas tengo para limitar el acceso a los equipos?

Una pregunta que me hacen algunos clientes es: de qué forma puedo limitar el acceso a los equipos, de forma que los usuarios únicamente accedan a los recursos necesarios para su trabajo.

"Como Responsables de Fichero, debemos establecer mecanismos para limitar el acceso a los sistemas de información"

Existen diversas maneras de identificación y autenticación del usuario en función del mecanismo o tecnología que se aplique.

Podemos clasificar los sistemas en estos tipos:

- Sistemas basados en algo que el usuario **conoce** (contraseña).
- Sistemas basados en algo que el usuario **posee** (DNI electrónico, token, etc.).
- Sistemas basados en una característica **física** del usuario, también denominados biométricos (reconocimiento de huella dactilar, voz, rostro, patrón ocular, etc.).
- Sistemas **mixtos**, que combinan dos o más de los descritos anteriormente.

En caso de que utilicemos el sistema más extendido, a través de contraseñas, para garantizar la seguridad se debe realizar una correcta gestión de las mismas:

- Aplicar una política de contraseñas "optimas", estableciendo para ello, una longitud mínima de 8 caracteres, combinando letras, números, mayúsculas y minúsculas, así como caracteres especiales (*$%&/-!=+).
- Evitar todas aquellas contraseñas deducibles por terceros y asociadas a parámetros comunes del usuario (fechas de nacimiento, nombre de familiares, matrículas de coches, aficiones, etc.).
- Establecer la periodicidad de cambio de las contraseñas a menos de 365 días.
- Limitar el número de intentos fallidos de acceso al sistema.