Boletín 07/12

LOPD EN LA EMPRESA

comSeveral
TIEMPO COSTE CALIDAD

LA LOPD EN EL DÍA A DÍA

¿Por qué están aumentando las amenazas hacia los datos personales?

Las amenazas y los incidentes de seguridad que afectan a los datos personales que las entidades almacenan **están aumentando notablemente** debido a los siguientes factores:

a) **Mayor dependencia** de los sistemas, servicios de información y tecnologías asociadas.

b) Complejidad y vulnerabilidad de la **tecnología** empleada.

c) **Volumen de información** cada vez más importante.

d) **Crecimiento exponencial** de las redes y usuarios interconectados.

e) **Aumento de las bases de datos** on-line.

f) Uso masivo del **cloud computing**.

g) **Inmadurez** de las nuevas tecnologías.

h) Alta disponibilidad de las **herramientas automatizadas para ataques** a la seguridad.

i) Técnicas de **ingeniería social**.

j) **Falta de concienciación** y formación del personal.

k) **Rentabilidad de los ataques**.

Contenido

A TENER EN CUENTA

En el determinado mercado negro, los datos personales son moneda de cambio.

SANCIONES DE LA AEPD

Pérdida de historia clínica

En la resolución de administraciones públicas PA/00016/2010 de la AEPD se detalla el **extravío de la historia clínica de un paciente** del Hospital Clínico Universitario de Valladolid, demostrándose que carece de las medidas de seguridad que la Ley exige al responsable del fichero.

Con fecha 26 de enero de 2010 tiene entrada en la AEPD un escrito de Dña. B.B.B. en el que declara que el Hospital Clínico Universitario de Valladolid ha extraviado su historia clínica, indicando que se dirigió por escrito al hospital solicitando su historia clínica. Manifiesta la denunciante que en la respuesta del Director Gerente del hospital se le informa de "que en dicho hospital se está a la espera de la localización de mi historia clínica, mencionándose en el indicado escrito una reconstrucción mínima y parcial de la misma con aquellos documentos últimos que se encuentran digitalizados".

En este caso concreto lo constatado es que la paciente solicitó el derecho de acceso a su historia clínica, que no se pudo satisfacer en ese momento porque no se localizó, que se solicitó que le entregase a su paciente una copia de su historia clínica en diez días y que el hospital manifiesta que cumplimentó este requerimiento transcurridos 20 días, sin que hasta la fecha se tenga constancia de la conformidad de su paciente que se solicitó en pruebas.

Resultado: DECLARAR que la Gerencia Regional de Salud de Castilla y León- Hospital Clínico Universitario de Valladolid ha infringido lo dispuesto en el artículo 9.1 de la LOPD, con una infracción tipificada como grave y REQUERIRLA para que implante las medidas que impidan que esto vuelva a ocurrir.

La organización debe implantar las medidas de seguridad recogidas en el Documento de Seguridad.

IMPORTANTE

Si esto mismo le ocurre a una clínica privada, en lugar de a un hospital público, el resultado hubiese sido, casi con seguridad, una fuerte sanción.

LA AEPD ACLARA

Acceso a los datos de personas fallecidas

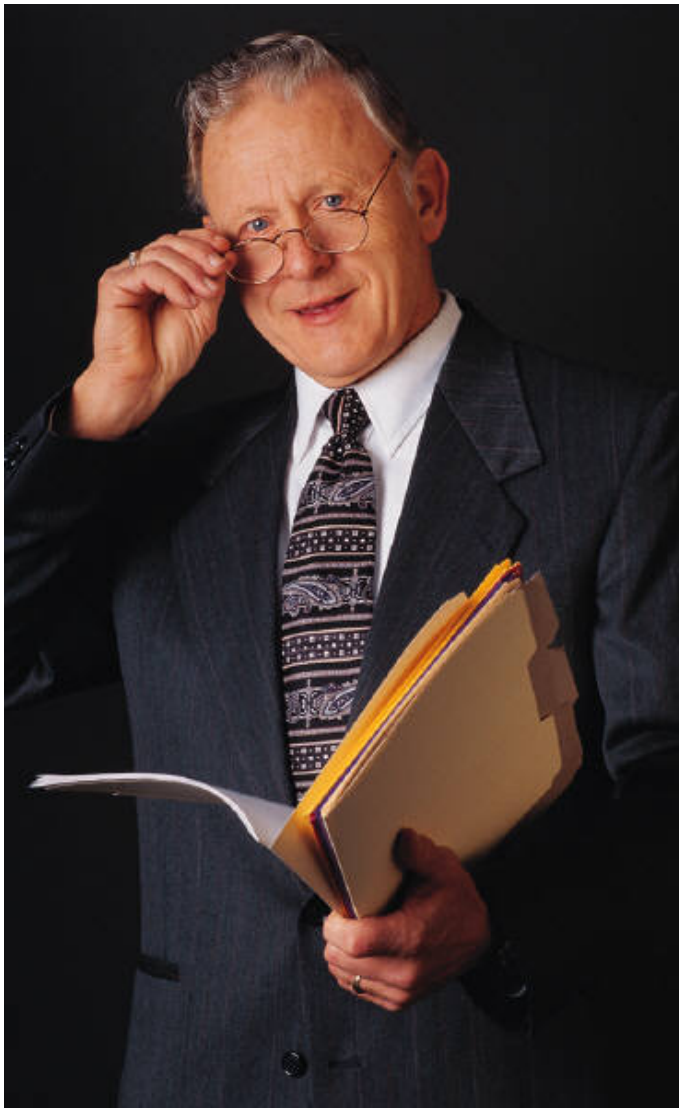
El informe 0523/2010 de la AEPD resuelve la consulta planteada sobre **la posibilidad de acceso por un investigador privado al expediente de un médico fallecido hace ya veinticinco años, y si puede fotocopiarlo o fotografiarlo**, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

De dicho informe jurídico se extrae lo siguiente:

a) **La protección** conferida por la Ley Orgánica 15/1999 **no se extiende a los datos de las personas fallecidas**, así lo indica expresamente el Reglamento de desarrollo de dicha Ley, aprobado por Real Decreto 1720/2007, por consiguiente el acceso a los datos a ellas referidas contenidos en los documentos que forman parte del Patrimonio Documental no se encuentra tutelado por dicha Ley Orgánica.

b) **Todo ello sin perjuicio de que la normativa que regule dicho Patrimonio establezca determinados plazos para permitir el acceso a sus datos.**

c) En concreto, la consulta de los documentos constitutivos del **Patrimonio documental Español** se atendrá a las de índole policial, procesal, clínico, o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, y no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que **haya transcurrido un plazo de 25 años desde su muerte** si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos.



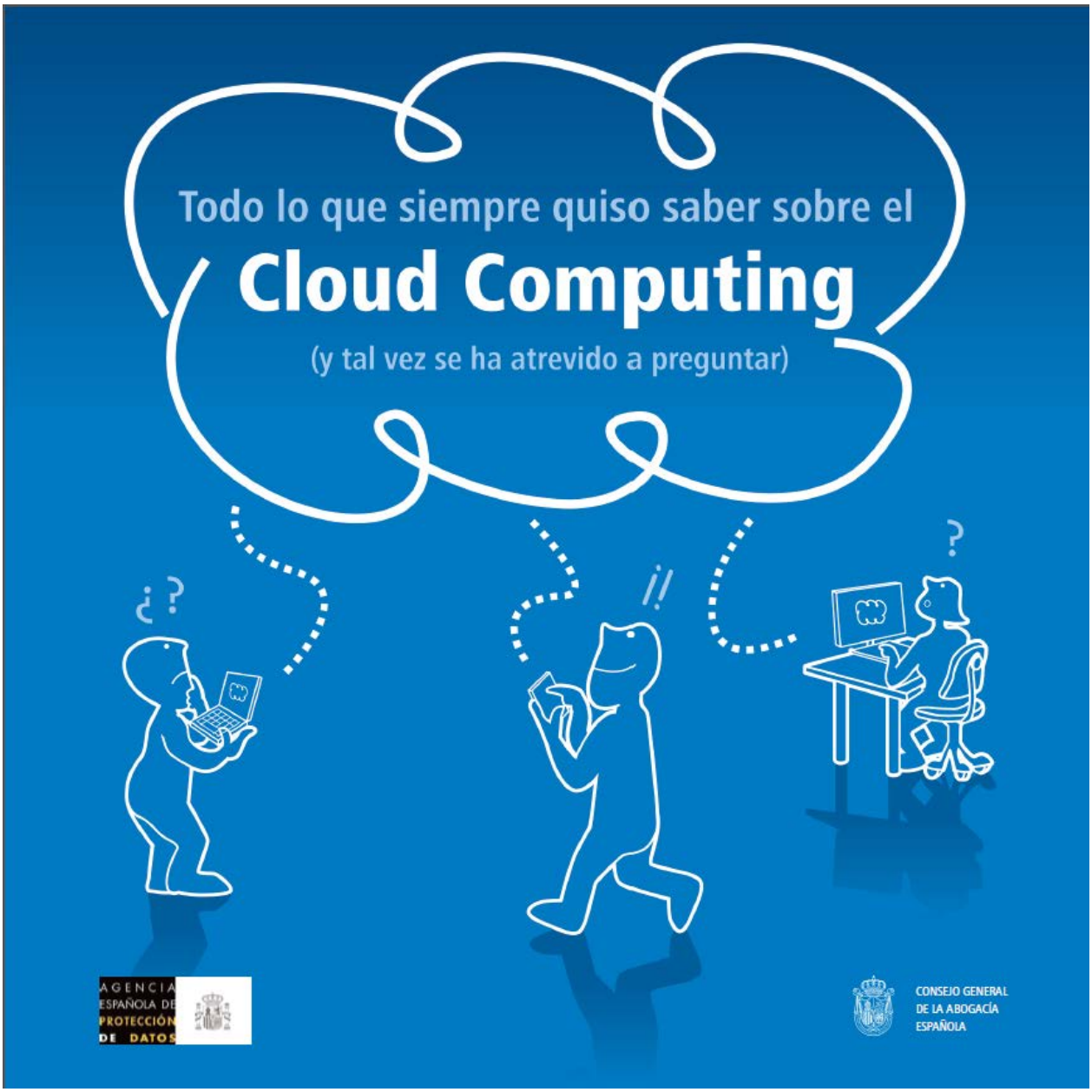
A TENER EN CUENTA

Siempre que se cedan o comuniquen datos hemos de ser extremadamente cautos.

ACTUALIDAD LOPD

La AEPD y CGAE presentan un informe sobre la utilización del cloud computing por los despachos de abogados.

Fuente: www.agpd.es



Puede acceder desde este enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/junio/Diptico_CLOUD.pdf

EL PROFESIONAL RESPONDE

¿Qué es la Ingeniería Social?

La Ingeniería Social es un conjunto de **acciones que se realizan con el fin de obtener información** a través de la manipulación de usuarios legítimamente autorizados para acceder a la misma.

Es un conjunto de trucos, engaños y artimañas que permiten confundir a una persona para que entregue información confidencial, ya sea la propia información, los datos necesarios para acceder a ésta o la forma de saltar la seguridad de un sistema.

Se dice que el único ordenador seguro es el que está desenchufado… en una caja fuerte, con una cerradura sellada y enterrada bajo hormigón… y aun así existen riesgos.

Los entendidos en Ingeniería Social, responden que siempre existirá un ser humano dispuesto a enchufarlo…

¿Cómo prevenirlo?

La mejor manera de estar prevenido, es tener el conocimiento sobre la Ingeniería Social. Para ello:

- Todo el **personal** debe ser **concienciado**, desde los usuarios al personal de limpieza.
- **No informar telefónicamente** a nadie de las características técnicas de la red, personal, etc.
- **Controlar el acceso físico** al sitio donde se encuentra los equipos informáticos y comunicaciones.

A TENER EN CUENTA

"El factor humano es el eslabón más débil de la seguridad de la información".