Boletín 09/12

LOPD EN LA EMPRESA

Aselio | PROTECCIÓN DE DATOS

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

**LA LOPD EN EL DÍA A DÍA**

# El Documento de Seguridad y las medidas de seguridad que contiene

El **Documento de Seguridad** describe las **medidas** que la organización tiene implantadas para **garantizar la seguridad** de los datos personales y cuyo objetivo es evitar:

- La pérdida de datos.
- La alteración no autorizada de los mismos.
- El acceso o difusión no autorizada.

Para ello, se debe tener en cuenta:

- La naturaleza de los datos almacenados.
- El estado de la tecnología.
- Los riesgos a que están expuestos dichos datos.

Es decir, no serán las mismas medidas de seguridad las que deberán implantarse para el tratamiento de datos meramente identificativos (nombre, apellidos, domicilio, etc.), que para el tratamiento de datos especialmente protegidos (salud, ideología, vida sexual, etc.).

**El tratamiento de datos más comprometidos requiere de más medidas de seguridad.**

**Contenido**



**A TENER EN CUENTA**

El responsable del fichero debe asegurarse de que las medidas de seguridad se aplican.

**SANCIONES DE LA AEPD**

# Error en el ensobrado de dos informes médicos

*El Documento de Seguridad debe detallar las medidas aplicadas.*

En el procedimiento sancionador PS/00159/2012 se puede ver la sanción que puede sufrir una empresa por **un error a la hora de realizar el ensobrado e intercambiar dos informes médicos**.

Con fecha de 12 de abril de 2011 tiene entrada en la AEPD un escrito de Dª. A.A.A. en el que declara que tras acudir en fecha 14/02/2011 para una **revisión ginecológica** a los **servicios de prevención de IBERMUTUAMUR**, el día 17/03/11 **recibió, vía postal, el resultado de su citología y el informe médico de la revisión realizada a Dª. B.B.B.**. Al día siguiente la denunciante contacta con ella a través de los datos de trabajo que, junto a los datos médicos, obraban en el informe. **Dª. B.B.B. le informó que, a su vez, ella disponía del informe de la denunciante**.

Aunque IBERMUTUAMUR **envió el Documento de Seguridad a la AEPD y alegó que ese incidente era un caso aislado**, ya que se realizan envíos de forma cotidiana y no ha habido nunca ningún problema, en el procedimiento sancionador se hace referencia a la sentencia de la Audiencia Nacional en la que se impone la **obligación de resultado**. Es decir, que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también **responsable de que las mismas se cumplan y se ejecuten con rigor**.

En definitiva, IBERMUTUAMUR, no actuó con la diligencia debida al **no adoptar las medidas de seguridad necesarias** y suficientes para impedir el acceso a la información de carácter personal.

**Resultado: Sanción de 4.000€ por infracción del art. 9.1 de la LOPD, relativo a la seguridad de los datos y tipificada como grave.**

**IMPORTANTE**

Las medidas de seguridad no solo deben estar en el Documento de Seguridad, han de implantarse de forma efectiva. El responsable ha de vigilar que se cumplan.

**LA AEPD ACLARA**

# Prevención del Blanqueo de Capitales y LOPD

El informe 0517/2010 de la AEPD resuelve la consulta planteada sobre **cuál es el régimen jurídico aplicable a las cesiones de datos en el seno de los Sistemas Institucionales de Protección SIP (mecanismo de consolidación de Entidades de crédito para su autoprotección), para el cumplimiento de las obligaciones de prevención del blanqueo de capitales y de la financiación del terrorismo, en relación a la LOPD.**

De dicho informe jurídico se extrae lo siguiente:

a) El artículo 24 de la Ley 10/2010 traspone al derecho español lo dispuesto en el artículo 28 de la Directiva 2005/60/CE, del Parlamento Europeo y del Consejo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo, cuyo apartado 1 dispone que **las entidades y personas sujetas a lo dispuesto en la presente Directiva, así como sus directivos y empleados, no revelarán al cliente de que se trate ni a terceros que se ha transmitido información** ni que está realizándose o puede realizarse una investigación sobre blanqueo de capitales o financiación del terrorismo.

b) No obstante, la Directiva, dispone que **esta prohibición no impedirá la comunicación entre entidades de los Estados miembros, o de terceros países**, siempre que cumplan las condiciones establecidas en el artículo 11, apartado 1, que pertenezcan al mismo grupo.

En conclusión, **la cesión de datos entre las entidades que conforman un sistema institucional de protección con la finalidad de prevención del blanqueo de capitales y la financiación del terrorismo se encuentra amparada por el art. 11.2 a) de la LOPD**, en conexión con el artículo 24.2 a) de la Ley 10/2010 y, particularmente, del artículo 28.3 de la Directiva 2005/60/CE.

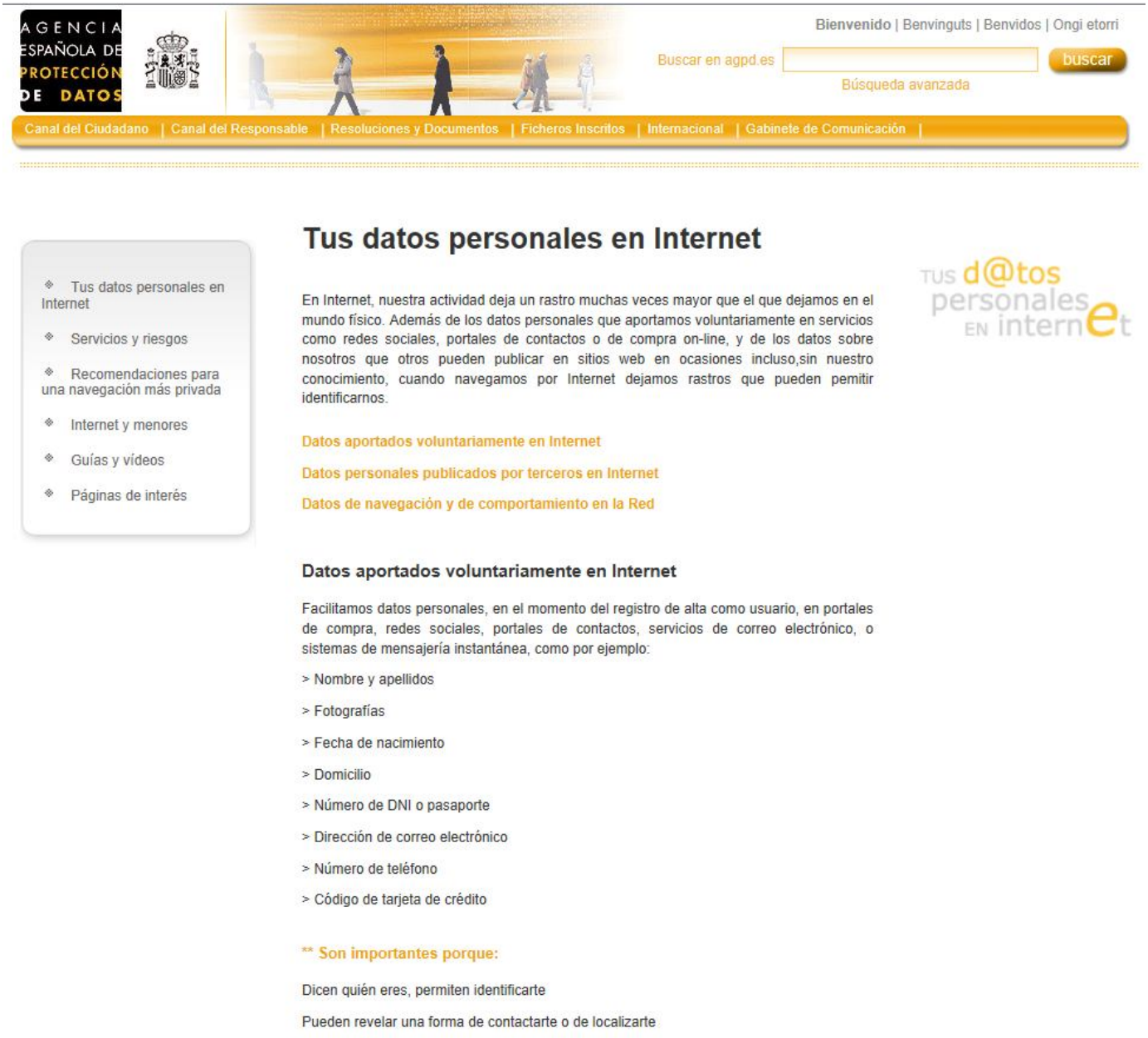
**A TENER EN CUENTA**

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

**ACTUALIDAD LOPD**

# Nueva sección con recomendaciones para usuarios de Internet en la web de la Agencia Española de Protección de Datos

*Fuente:* [www.agpd.es](http://www.agpd.es)




Puede acceder desde este enlace:

http://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2012/tus_datos_personales_en_internet-ides-idphp.php

**EL PROFESIONAL RESPONDE**

# ¿Qué ocurre si no puedo aplicar todas las medidas de seguridad a todos los datos personales que trato?

Una de las obligaciones que tiene el responsable del fichero es **proteger los datos personales** que trata.

Los riesgos a que están expuestos los ficheros pueden venir, tanto de la acción humana, como de circunstancias naturales, o de accidentes fortuitos.

Resulta necesario que el responsable del fichero adopte las medidas adecuadas y necesarias para garantizar la protección de datos de carácter personal para evitar su destrucción, pérdida, alteración, difusión o acceso no autorizado.

## FICHEROS QUE NO REUNAN LAS CONDICIONES DE SEGURIDAD

**No se registrarán datos** de carácter personal en ficheros que no reúnan las condiciones requeridas respecto a su integridad y seguridad y las de los centros de tratamiento, locales, equipos, sistemas y programas.

Es decir, que **no tenemos excusa**. Si tratamos datos personales hemos de **aplicar las medidas de seguridad** descritas en el Documento de Seguridad.

**A TENER EN CUENTA**

El responsable del fichero debe asegurarse de que las medidas de seguridad se aplican.