

LA LOPD EN EL DÍA A DÍA

¿Qué he de mantener actualizado en el Documento de Seguridad?

La LOPD establece que el Documento de Seguridad deberá mantenerse actualizado, de forma que **refleje** en todo momento la **realidad de la organización**.

A tal efecto, deberemos **estar atentos a los siguientes cambios** para actualizar el Documento de Seguridad:

- **Usuarios** que acceden a los ficheros.
- Modificaciones en los **procedimientos**.
- **Encargados** del tratamiento y servicios prestados.
- **Equipamiento** informático.
- Actualizaciones/instalaciones de **software**.
- **Incidencias** que se produzcan.
- **Personas autorizadas** para salidas de soportes, uso de portátiles, etc.
- **Administradores** de los ficheros y responsables de seguridad.
- **Comenzamos a recoger datos** que antes no se recogían (ej. Correo electrónico de los clientes).
- **Nuevos soportes** que deban incluirse en el inventario de soportes y documentos.

Contenido

¿Qué he de mantener actualizado en el Documento de...	1
Sanción no atender requerimiento de la AEPD	2
Cesión de datos de profesores en web	3
La AEPD publica la guía “Recomendaciones a usuarios...	4
¿Cómo gestiono las altas y bajas de los usuarios en los...	5



A TENER EN CUENTA

Debe realizarse una revisión completa del Documento de Seguridad al menos **una vez al año**, para verificar que la información contenida está actualizada.

SANCIONES DE LA AEPD**Sanción no atender requerimiento de la AEPD**

En el procedimiento sancionador [PS/00660/2010](#) de la AEPD podemos ver la sanción que puede sufrir una entidad por **no atender un requerimiento de la Agencia Española de Protección de Datos** para realizar **comprobaciones de oficio** sobre el cumplimiento de la LOPD.

Con fecha 26 de marzo de 2010, el Director de la AEPD envió al SANATORIO SAN JORGE DE ALOY el requerimiento relativo al Informe de cumplimiento de la LOPD en Hospitales y se requería que lo cumplimentase antes del 31 de mayo de 2010.

El 18 de junio de 2010, se remitió un segundo requerimiento al no haberse recibido contestación al primero, para que procediera a la cumplimentación del citado informe antes del 31 de julio de 2010.

El 25 de noviembre de 2010, el Director de la AEPD acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas por presunta infracción del art. 37.1.a) de la LOPD.

La entidad alegó que el primero no fue atendido por un problema interno y el segundo no tiene constancia de su recepción y no fue atendido por desconocimiento.

Durante la instrucción del procedimiento el SANATORIO SAN JORGE DE ALOY cumplimentó el Informe de cumplimiento de la LOPD en centros hospitalarios y le fue remitido a la AEPD para su conocimiento.

Resultado: Sanción de 3.000 € por vulneración del artículo 37.1 de la LOPD.

Todo el personal de la empresa ha de ser diligente en el cumplimiento de la LOPD.

**IMPORTANTE**

Ante un requerimiento de la AEPD (el que sea) lo peor que puede hacer una entidad es dejarle sin contestación.

LA AEPD ACLARA

Cesión de datos de profesores en web

El informe [0427/2010](#) de la AEPD resuelve la consulta planteada sobre si la consultante puede proceder a **publicar en la página web de la Universidad los datos de contacto de sus profesores** consistentes en el número de teléfono y correo electrónico de la Universidad **sin su consentimiento**, con la finalidad de favorecer la actividad docente a través de la interrelación con los alumnos

De dicho informe jurídico se extrae lo siguiente:

- a) La comunicación planteada implica la existencia de una **cesión de datos** de carácter personal.
- b) Toda cesión de datos debe obtener el **consentimiento previo** del interesado salvo que se dé cualquiera de los supuestos del artículo 11.2 de la LOPD.
- c) El RD1720/2007, en su art. 2.2 establece que **no será de aplicación** la LOPD a los tratamientos de datos referidos a las **personas jurídicas** ni a los ficheros que se limiten a incorporar datos de las personas físicas que presten sus servicios en aquellas consistentes únicamente en su nombre y apellidos, funciones o puestos, dirección postal, teléfono y fax profesionales. **Siempre que la finalidad sea contactar con la entidad y no con la persona.**
- d) Por ello, si los datos de los profesores aparecen exclusivamente vinculados a su actividad como docentes, en su entorno profesional, no están esos datos dentro del ámbito y **no sería necesario el consentimiento para la cesión.**

**A TENER EN CUENTA**

La cesión de datos es una de los principios de la LOPD que más dudas suscitan.

ACTUALIDAD LOPD

La AEPD publica la guía “Recomendaciones a usuarios de Internet”



Fuente: www.agpd.es



Puede descargarse el manual aquí:

http://www.agpd.es/portaIwebAGPD/canaIdocumentacion/publicaciones/common/pdfs/guia_recomendaciones_internet_052009.pdf

EL PROFESIONAL RESPONDE

¿Cómo gestiono las altas y bajas de los usuarios en los equipos informáticos para que no se me escape nada?

Los procedimientos de control de acceso deben tener en cuenta el **ciclo de vida del usuario**, desde su alta en el sistema, hasta la baja en el mismo.

Para ello, se debe redactar un procedimiento o política de registro de altas y bajas de usuarios, cobrando mayor importancia su estricto cumplimiento, cuantos más usuarios accedan al sistema.

La política debe cumplir, entre otros los siguientes extremos:

- Asignar un **identificador único** por usuario, no compartiendo dicho identificador diferentes usuarios.
- En caso de **baja definitiva** de un usuario, eliminar inmediatamente sus derechos de acceso.
- En caso de **baja temporal**, bloquear su identificador.
- **Revisar periódicamente** la lista de usuarios con la de personal, eliminando usuarios redundantes y los que no están en la lista, así como revisar los recursos a los que tienen acceso.
- **Cotejar la lista de usuarios** anterior con la lista de usuarios y accesos permitidos del Documento de Seguridad.

**IMPORTANTE**

La lista de usuarios con acceso a los recursos debe **coincidir** con la lista de usuarios y accesos del Documento de Seguridad.