

## Auditoría sobre el Cumplimiento de la LOPD

### Situación Actual

Algunas empresas, conscientes de la necesidad de cumplir con la normativa sobre protección de datos, ya han tomado medidas para su adecuación a la Ley Orgánica de Protección de Datos Personales (LOPD).

El Reglamento de desarrollo de la LOPD, entre otras muchas exigencias, establece la obligatoriedad de realizar una auditoría al menos cada 2 años para verificar el cumplimiento de las medidas de seguridad establecidas en el mismo. Estas medidas son de índole técnica, jurídica y organizativa. También son necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de datos de carácter personal.

La adecuación a la LOPD no se debe considerar completa por la simple implantación inicial de las medidas propuestas en la misma, valorando este hecho como suficiente para evitar sanciones. En ESA Security recomendamos que la auditoría se haga con más fre-

cuencia de la legalmente prevista en la normativa, pues nos encontramos que a menudo las circunstancias internas de la empresa cambian con respecto a las que eran en el periodo de la adecuación o de revisiones posteriores.

### Nuevo Reglamento

El nuevo Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, cuya entrada en vigor fue el 19 de abril de 2008, prevé una ampliación y regulación menos generalista de las obligaciones sobre protección de datos.

En concreto y entre otros aspectos, el Reglamento ha venido a:

- aclarar su ámbito objetivo de aplicación;
- establecer una regulación del modo de captación del consentimiento, por ejemplo, en el caso de los menores o de los servicios de comunicaciones electrónicas;
- prever criterios específicos para determinados ficheros de titularidad pri-

vada, como los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial;

d) ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que correspondan en cada caso y en la revisión de las mismas;

e) ordenar con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del Documento de Seguridad, de obligada tenencia en las empresas.

### Servicios relativos a la Auditoría LOPD

La auditoría de una empresa o institución para verificar su nivel de cumplimiento de la normativa, suele tener cierto grado de dificultad y requiere la acción combinada de especialistas en diversos campos de actuación: jurídico, técnico y organizativo. Esto induce a las empresas a plantearse la externalización de estos servicios de control y vigilancia de cumplimiento. Si éste es su caso, ESA Security le puede ofrecer su larga experiencia en la prestación de

los siguientes servicios:

#### Revisión de Situación Técnica

A través de un Informe Ejecutivo se expone el grado de cumplimiento de las medidas contempladas en el Reglamento, para aquellos ficheros de nivel medio y alto declarados por la empresa.

#### Revisión de Situación General

A través de un Informe Ejecutivo se expone el grado de adaptación de la empresa a la normativa sobre Protección de Datos verificando el cumplimiento de los controles, procedimientos e instrucciones en materia de seguridad de datos, así como de las medidas contempladas en el Reglamento.

#### Auditoría

El objetivo es garantizar el cumplimiento de las medidas técnicas, organizativas y jurídicas que garanticen la seguridad de los datos dentro de la empresa.

#### Mantenimiento

Este servicio está orientado a las empresas que quieren cumplir con sus obligaciones dedicando al mismo tiempo el menor tiempo posible de sus empleados. Incluye la revisión de los ficheros declarados, de los contratos, políticas y procedimientos, así como la actualización del documento de seguridad, las consultas jurídicas y la auditoría bienal.

#### Beneficios

- Ganar confianza frente a terceros.
- Eliminación de muchos riesgos propios del negocio.  
Durante la auditoría se pueden encontrar debilidades tales como ficheros informáticos desprotegidos que pueden ser copiados, robados o dañados, procedimientos de respaldo inexistentes o una protección insuficiente frente a los piratas informáticos.
- Mejora de la productividad.  
Como consecuencia de la auditoría, se suelen encontrar procesos innecesarios o ineficientes que pueden mejorarse sustancialmente con muy poco esfuerzo.
- Reducción del riesgo de sanciones.  
La implantación de medidas preventivas proporciona una mayor seguridad de cumplimiento por parte de la empresa de la normativa sobre protección de datos, consiguiendo por ello un menor riesgo de posibles sanciones de la AEPD y de las denuncias de particulares ante este organismo.  
No realizar la auditoría es un incumplimiento grave duramente sancionado.
- Reducción del riesgo de mala imagen.  
Cumpliendo con la auditoría obligatoria por la LOPD se reduce el riesgo de una mala publicidad. Muy a menudo éste es un factor de motivación superior a la propia sanción.

- Reducción del alto riesgo de las responsabilidades de los directivos.

En última instancia, son los responsables de cada departamento los que responderán del cumplimiento de la LOPD ante su corporación.

Con la auditoría, cada directivo llega a conocer su propia responsabilidad, los riesgos de la misma, así como si está asumiendo, por desconocimiento, una responsabilidad mucho mayor de la que le corresponde.

#### Sobre ESA Security

ESA Security es una consultora especializada únicamente en la Seguridad de la Información que realiza frecuentemente con éxito la preparación de empresas para que consigan su Certificación ISO 27001 sobre la Seguridad de la Información con cualquier certificadora acreditada por ENAC o UKAS. Sus profesionales están altamente cualificados, incluyendo certificaciones CGEIT, CISM y CISA, y lo más importante: con la experiencia práctica de haber conseguido Certificaciones ISO 27001 y haber realizado en múltiples ocasiones Planes Directores de Seguridad, Planes de Continuidad de Negocio, Análisis y Gestión de Riesgos, Proyectos de Hacking Ético, Formación en Seguridad, Adecuaciones y Auditorías LOPD y servicios relativos a la Seguridad de la Información en general.