Volumen 1, nº 1

P C N E T

Enero 2009

De interés especial:

- Tanto el concepto de sistema de información como recurso pueden referirse a ficheros manuales.
- Todos los ficheros creados con posterioridad a la entrada en vigor del RLOPD (20 de abril de 2008) deberán haber implantado todas las medidas de seguridad exigidas por el RLOPD.

Contenido:

La Seguridad en la Protección de Datos Personales

La LOPD y su nuevo reglamento (Ley 15/1999 y R.D. 1720/2007)

¿Cómo debe el responsable del fichero garantizar la seguridad de los datos personales que gestiona?

El Responsable del Fichero, y en su caso, el Encargado del Tratamiento" están obligados a adoptar la medidas de **índole técnica y organizativas** necesarias para garantizar la seguridad de los datos de carácter personal y **evitar su alteración, pérdida, tratamiento o acceso no autorizado.**

La Ley 15/1999 de Protección de Datos de Carácter Personal (LOPD) proporciona un sistema de objetivos y criterios en materia de seguridad de los datos personales compatible con los principios y criterios generalmente aceptados en el mundo de la seguridad de los sistemas de información y que, aplicando de modo sistemático y complementado en lo necesario con las reglas, técnicas y procedimientos imperantes en dicho mundo, puede permitir discernir al aceptabilidad del conjunto de medidas de protección adoptadas en cada caso, hasta tanto no se plasmen dichos criterios en una regulación detallada como la prevista en los apartados 2 y 3 del Art. 9 de la Ley.

La regulación de que habla el Art. 9 de la LOPD se desarrolló en el **Reglamento de la LOPD,** donde se detallan las medidas de seguridad para cada caso (R.D. 1720/2007).

La combinación de los factores "**datos a proteger" y "riesgo a que están expuestos",** es la que determina el daño esperable que se derivaría de una inadecuada protección, y por lo tanto el nivel de protección exigible.

"La confidencialidad impide el tratamiento o acceso no autorizados a los datos personales ."

La responsabilidad, en caso de vulnerarse, recae directamente sobre la entidad responsable del fichero.

Desarrollo del principio de seguridad en el RLOPD

La regulación del principio de seguridad se desarrolla en el Título VIII, Capítulos I y II del Reglamento de la LOPD.

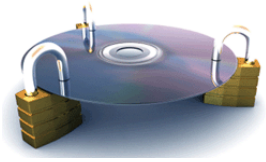
Se establecen 3 niveles de seguridad: **básico, medio y alto.** Como novedades cabe destacar que el RLOPD tiene en cuenta diferentes factores para la anterior clasificación:

- Tipo y naturaleza de los datos.
- Tipo de actividad del responsable del fichero.
- Objeto social del responsable del fichero o naturaleza pública o privada del mismo.

También se implica en la seguridad las prestaciones de servicios y accesos por cuenta de terceros, responsabilizando en algunos casos al **Encargado del Tratamiento**.

Especial atención a la elaboración del **documento de seguridad** que habrá de recoger las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente y que será de **obligado cumplimiento** para el personal con acceso a los sistemas de información.

Otra de las novedades del RLOP es que hace referencia a datos de carácter personal, esto incluye tanto ficheros automatizados como ficheros **no automatizados.**



Plazos de aplicación de medidas de seguridad

El RLOPD entró en vigor el 20 de abril de 2008, pero teniendo en cuenta las novedades respecto al anterior reglamento, se establecieron unos plazos para su aplicación.

Para ficheros automatizados:

Como regla general un año desde la entrada en vigor. **Excepciones:** 18 meses para ficheros de datos derivados de actos de violencia de género y datos de tráfico y localización en ficheros de operadores que presten servicios de comunicaciones electrónicas o exploten redes públicas de comunicaciones.

Para ficheros no automatizados:

Ficheros de nivel básico: 1 año.

Ficheros de nivel medio: 18 meses.

Ficheros de nivel alto: 2 años

“La integridad evita la alteración indebida de los datos personales.”

Medidas de seguridad

Sin duda, la implantación de las medidas de seguridad exigidas por el Reglamento constituye una de las principales fuentes de obligaciones para el responsable del fichero y, en su caso, para el encargado de tratamiento.

Un estudio realizado por el INTECO en 2007 revela que sólo el 17,7% de las empresas realizan auditorías de seguridad y sólo un 23,4% disponen de Documento de Seguridad.

Podríamos decir que sin un cumplimiento adecuado de las medidas de seguridad establecidas en la normativa vigente, **no resulta legítimo** ningún tratamiento de datos personales.

Así, el Art. 9 de la LOPD dice:

“No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas”.

Es especialmente destacable la regulación de un conjunto de medidas destinadas a los ficheros y tratamientos automatizados y no automatizados (ficheros manuales). El RLOPD aplica 3 niveles de seguridad para los ficheros automatizados y para los no automatizados. Estos niveles se clasifican en: **básico, medio y alto.**

En conclusión:

Se trata de un marco que pretende garantizar un tratamiento adecuado para todos los datos personales, independientemente del soporte en el que éstos se encuentren o de la finalidad a la que se destinen.

El objetivo fundamental es que, en todo caso, los datos están protegidos de cualquier posible incidencia que pueda provocar su pérdida, alteración o acceso no autorizado (tanto interno como externo).

El RLPD es una evolución del anterior reglamento que con la experiencia de los años nos pone de manifiesto dos importantes facetas:

- Un incremento de las obligaciones que los responsables de los ficheros deberán asumir. Y,
- La adecuación de las obligaciones en función de las posibilidades reales de implantación de los responsables.

Por otra parte, no olvidemos la regulación detallada de las medidas de aplicación a los ficheros de carácter no automatizado, ya que va a implicar la aparición de nuevas obligaciones para estos responsables.

El Documento de Seguridad

El Art. 88.1 del RLOPD dispone: "*El responsable del fichero o tratamiento elaborará un Documento de Seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información".*

En el redactado del artículo cabe destacar que dice "fichero o tratamiento" sin especificar si éstos son automatizados o manuales.

El Documento de Seguridad podrá ser:

- Único y comprensivo para todos los ficheros o tratamientos, o
- Individualizado para cada fichero o tratamiento.

También se podrán elaborar distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento o atendiendo a criterios organizativos del responsable.

En todo caso, el Documento de Seguridad, tendrá carácter de documento interno de la organización.

Deberá contener:

* Ámbito de aplicación del documento.
* Medidas, normas, procedimientos de aplicación, reglas y estándares que garanticen el nivel de seguridad.
* Funciones y obligaciones del personal.
* Estructura de los ficheros.
* Procedimiento de las incidencias.
* Procedimiento de copias de respaldo y recuperación.
* Medidas para transporte de soportes y documentos, así como su destrucción.

"La disponibilidad previene de la pérdida de datos personales."

La auditoría de medidas de seguridad

Obligación de auditar en el RLOPD: Art. 96.

"A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos ***cada dos años****, a una auditoría* ***interna o externa*** *que verifique el cumplimiento del presente título".*

En cuanto a los ficheros **no automatizados**, *"… se someterán, al menos cada dos años a una auditoría interna o externa que verifique el cumplimiento del presente título".*

La obligación de auditar se puede analizar desde distintas perspectivas:

⇒ Alcance de la Auditoría.

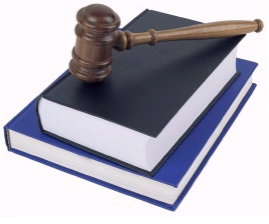
⇒ Tipos de auditoría previstos en la norma (interna o externa).

⇒ Auditoría de medidas de seguridad y auditoría informática.

Sanciones por incumplimiento de la LOPD.

Artículo 45 LOPD. Tipo de sanciones.

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.
2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.
3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.
4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.
6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.
7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.



P C N E T

Soluciones informáticas para empresas y particulares.

Teléfono: 616 48 92 91
Correo: info@pcnet.com.es
Barcelona

http://www.pcnet.com.es

Procesos de apoyo a la Norma UNE-EN ISO 9001

Confección de los documentos de los procesos de apoyo para la correcta aplicación de un **sistema de gestión de calidad** (Norma ISO 9001): Comunicaciones internas y externas, seguridad informática y equipos informáticos.

Legislación informática

Asesoramiento para la aplicación de la LOPD.

Redacción del Documento de Seguridad que obliga la LOPD (Ley 15/1999)

Aplicación de la ley de Internet. (Ley 34/2002)

Firma electrónica y cumplimiento de la Ley 59/2003

Administración de redes

Mantenimiento de equipos

Seguridad informática

Formación de usuarios

Derecho informático (LOPD, LSSI, etc.)

Posicionamiento Web

Adaptación ISO 9001

La Agencia Española de Protección de Datos

Regulación Normativa:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria).
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

Naturaleza:

- Ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada.
- Actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones

Estructura