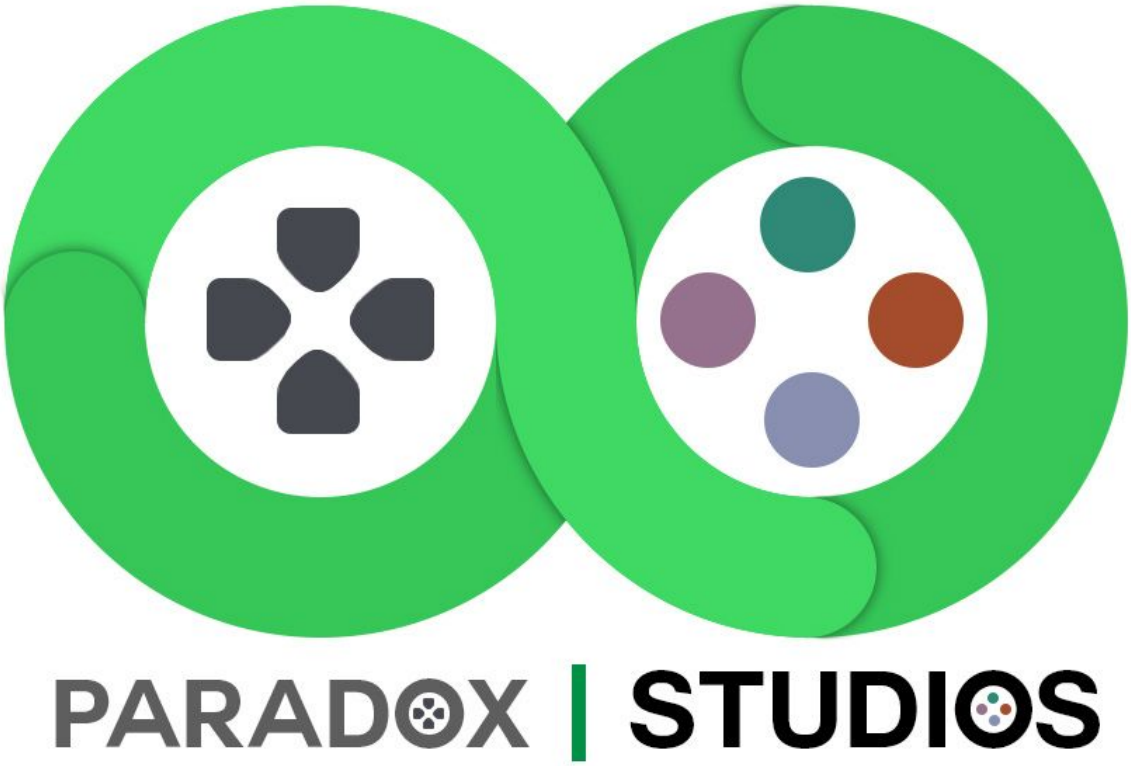
# La Ley Orgánica de Protección de Datos (LOPD)




***Paradox Studios:***
Moltó Ferré, Enrique
Muñoz Periñán, José Luis
Pérez Cristo, Rubén
Rebollo Berná, Antonio
Zamora Pastor, Julio

# Índice


**1- La agencia de protección de datos** **2**

1.1 - ¿Qué es la agencia de protección de datos? 3

1.2 - Historia 3

1.3 - Funciones de la Agencia Española de Protección de Datos 5

1.4 - Organigrama y partes de la agencia 7

**2- Registro de ficheros** **9**

2.1 – Definiciones básicas 9

2.2 – Ficheros sometidos a inscripción y proceso de registro 9

2.3 – El sistema NOTA 10

2.4 – Formatos y especificaciones XML 10

**3- El documento de seguridad** **12**

3.1 – ¿Qué es el documento de seguridad? 12

3.2 – Artículo 9 de la Ley Orgánica 15/1999 12

3.3 – Artículo 88.1 del Real Decreto 1720/2007 12

3.4 – ¿Qué debe contener el documento de seguridad? 12

3.5 – Actualización del documento de seguridad 14

3.6 – Consecuencias de no disponer de un documento de seguridad 14

3.7 – Modelo del documento de seguridad 14

**4- El personal involucrado** **17**

4.1 – Responsable del fichero 17

4.2 – Afectado o interesado 18

4.3 – Encargado del tratamiento 18

4.4 – Usuario 19

4.5 – Responsable de seguridad 19

**5- Control de accesos** **21**

5.1 – ¿Qué es el control de accesos? 21

5.2 – ¿Para que se usa? 21

5.3 – ¿De que esta compuesto? 21

5.4 – Que tipos hay y que pasos los componen. 22

5.5 – Objetivos del control de acceso 23

5.6 – Los niveles de seguridad 23

5.7 – ¿Qué es un fichero automatizado y un fichero no automatizado? 23

5.8 – Real Decreto 1720/2007 24

5.9 – Medidas de seguridad para ficheros y tratamientos automatizados 24

5.10 – Medidas de seguridad para ficheros y tratamientos no automatizados 27

5.11 – Tabla resumen 28

**6- Gestión de soportes y documentos 29**

6.1 – Aclaraciones básicas 29

6.2 – Ficheros automatizados 29

Medidas de seguridad de nivel básico: 29

Medidas de seguridad de nivel medio: 29

Medidas de seguridad de nivel alto: 30

6.3 – Ficheros no automatizados 30

Medidas de seguridad de nivel alto: 30

6.4 – Tabla resumen 31

**7- Copias de seguridad 32**

7.1 – ¿Qué son las copias de seguridad? 32

7.2 – ¿Obligaciones de la LOPD en materia de copias de seguridad? 32

7.3 – Artículos relacionados con las obligaciones de la LOPD 33

7.3 – Sanciones 34

**8- Seguimiento y control (Auditoría LOPD) 35**

8.1 – ¿Qué es una auditoría de protección de datos? 35

8.2 – Objetivos de la auditoría 36

8.3 – ¿Qué puede hacer la auditoría? 36

8.4 – Pasos a seguir en un auditoría 36

8.5 – Sanciones 37

**Referencias: 38**

Punto 1 - La agencia de protección de datos: 38

Punto 2 - Registro de ficheros: 38

Punto 3 - El documento de seguridad: 38

Punto 4 - El personal involucrado: 39

Punto 5 - Contro de accesos: 39

Punto 6 - Gestión de soportes y documentos: 40

Punto 7 - Copias de seguridad: 40

Punto 8 - Seguimiento y control (Auditoría LOPD): 40

# 1- La agencia de protección de datos

## *1.1 - ¿Qué es la agencia de protección de datos?*

La agencia de protección de datos se define así misma cómo "la **autoridad estatal de control** independiente encargada de velar por el **cumplimiento de la normativa sobre protección de datos**. Garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos".

La Agencia es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se relaciona con el Gobierno a través del Ministerio de Justicia.

## *1.2 - Historia*

El artículo 18.4 de la Constitución española afirma lo siguiente:

**"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."**

**http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2**

Además, el Tribunal Constitucional proclamó que el derecho a la protección de datos es un verdadero derecho fundamental, autónomo y claramente diferenciado de los demás.

El Convenio 108 del Consejo de Europa de 1981 prevé la existencia de una autoridad independiente que vele por el derecho a la protección de datos. Su configuración más acabada queda constatada en la Directiva 95/46/CE, encargada de la protección de datos personales de las personas físicas y la circulación de dichos datos. Esta Directiva sigue presente en el marco normativo general de la UE, aunque se encuentra en estado de revisión.

https://www.urjc.es/images/proteccion_datos/B.4-cp—Directiva-95-46-CE.pdf (Directiva 95/46)

*Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales.* (Considerando número 62 de la Directiva 95/46, referenciada en el hipervínculo superior).

*Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.* (Artículo 28.1 de la Directiva 95/46)

Como reza el artículo 28.1 de la Directiva 95/46, estas instituciones deberán ejercer sus funciones con total independencia, así pues, en España se adoptó el modelo propuesto en el Convenio 108 e

incorporó una institución independiente que se encargaría de velar por el cumplimiento de la normativa de protección de datos.

La Agencia Española de Protección de Datos goza de un presupuesto propio y plena autonomía funcional. La AEPD se creó en 1992 y comenzó a funcionar en 1994.

La representación de la Agencia la ostenta su Director que es elegido de entre los miembros del Consejo Consultivo de la Agencia Española de Protección de Datos. Su nombramiento se produce mediante Real Decreto a propuesta del Ministro de Justicia. Su primer director fue Juan José Martín-Casallo López(1993-1998), y su actual directora es Mar España Martí, que ostenta el cargo desde 2015.

**Agencias autonómicas**

Como refleja el artículo 28.1 de la Directiva 28.1, un Estado de la UE puede disponer de *una o más autoridades públicas que se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.* Esto quiere decir que un solo Estado puede tener varias instituciones públicas, así pues, se crearon tres agencias autonómicas:

1. En Madrid, en el año 2001.

2. En Cataluña, en el año 2003.

3. En el País Vasco, en el año 2004.

La Agencia de Protección de Datos de la Comunidad de Madrid fue eliminada en el año 2013 y todas sus funciones pasaron a ser asumidas por la **Agencia Española de Protección de Datos.** Por lo tanto actualmente solo existen dos agencias autonómicas, la **Autoridad Catalana de Protección de Datos** y la **Agencia Vasca de Proteccion de Datos.** Estas ejercen las funciones de control para los ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, en cambio, los ficheros privados de Cataluña y el País Vasco son competencia de la Agencia Española de Protección de Datos.

## *1.3 - Funciones de la Agencia Española de Protección de Datos*

La Agencia se encarga de velar por el cumplimiento de la legislación sobre protección de datos y su aplicación.

Las funciones de la Agencia en relación a los actos/actores involucrados:

1. **En relación a los afectados:**

   - Atender a sus peticiones y reclamaciones.
   - Informar de los derechos de la Ley.
   - Promover campañas de difusión.
   - Velar por la publicidad de los dicheros de datos de carácter personal.

2. **En relación con quienes tratan datos:**

   - Emitir las autorizaciones pertinentes.
   - Requerir medidas de corrección.
   - En caso de ilegalidad, ordenar el cese en el tratamiento y la cancelación de los datos.
   - Ejercer la potestad sancionadora en los términos previstos en el Título VII de la Ley Orgánica de Protección de Datos.
   - Recabar de los responsables de los ficheros la ayuda e información que precise para el ejercicio de sus funciones.
   - Autorizar las transferencias internacionales de datos.

3. **En la elaboración de normas:**

   - Informar preceptivamente los Proyectos de normas de desarrollo de la Ley Orgánica de Protección de Datos.
   - Informar los Proyectos de normas que incidan en materia de protección de datos.
   - Dictar las instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica de Protección de Datos.
   - Dictar recomendaciones de aplicación de las disposiciones legales y reglamentarias en materia de seguridad de los datos y control de acceso a los ficheros.

4. **En materia de telecomunicaciones:**

   - Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas (spam).
   - Recibir las notificaciones de las eventuales quiebras de seguridad que se produzcan en los sistemas de los proveedores de servicios de comunicaciones electrónicas.

5. **Otras funciones:**

   - Cooperación con diversos organismos internacionales y con los órganos de la Unión Europea en materia de protección de datos.
   - Representación de España en los foros internacionales de la materia.
   - Control y observancia de los dispuesto en la Ley reguladora de la Función Estadística

Pública.

- Elaboración de una Memoria Anual, que es presentada por el Director de la Agencia ante las Cortes.

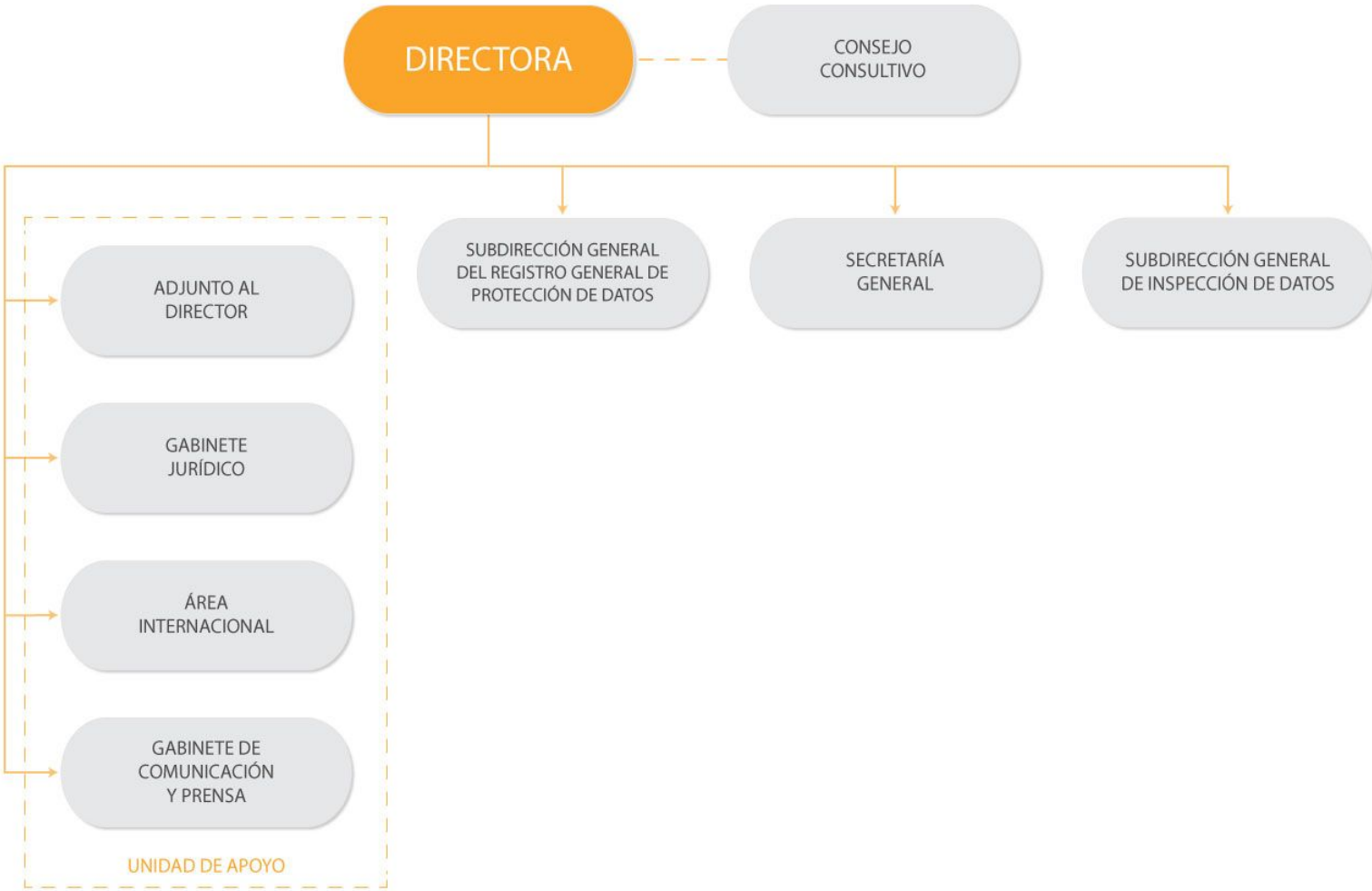
**Carta de servicios:**

Los Órganos, Organismos y Entes Públicos y otras Entidades de la Administración General del Estado informan a los ciudadanos y usuarios sobre los servicios que tienen encomendados y los derechos que les asisten a través de un documento denominado **Carta de Servicios.**

La Carta de Servicios que proporciona la Agencia Española de Protección de Datos se puede conseguir a través del siguiente **enlace:**

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/CartaServiciosAEPD.pdf

## *1.4 - Organigrama y partes de la agencia*




1. **Directora:**

**<u>Doña Mar España Martí.</u>**

La directora representa a la Agencia y sus actos se consideran como actos de la Agencia. Sus resoluciones ponen fin a la vía administrativa y son recurribles ante la Sala de lo Contencioso de la Audiencia Nacional.

Su nombramiento lo realiza el Gobierno mediante Real Decreto por el Consejo Consultivo y a propuesta del Ministro de Justicia. Su mandato es de cuatro años.

La directora no puede recibir instrucciones de ningún poder o autoridad y ejerce sus funciones con plena independencia y objetividad.

2. **Consejo Consultivo:**

Es el órgano de asesoramiento del Director, siendo este elegido entre sus miembros, esta compuesto por 10 miembros nombrados por un periodo de cuatro años. Es presidido por el director de la Agencia.

El Consejo Consultivo se reúne cuando lo convoca el director y, como mínimo, cada seis meses. Emite informes en todas las cuestiones que le someta el director, pudiendo realizar propuestas relacionadas con la protección de datos.

3. **Inspección de datos:**

**Subdirector general de inspección de datos: Pedro Colmenares Soto**

Se encarga de tramitar los procedimientos relativos al ejercicio de la potestad sancionadora que tiene a cargo la Agencia sobre protección de datos, spam y cookies y llamadas automáticas sin intervención humana o mensajes de fax con fines comerciales. Sintetizando, ejerce la función inspectora.

También tutela los derechos de acceso, rectificación, cancelación y oposición de los ciudadanos (ARCO).

4. **Secretaría general**

**Subdirectora general, secretaría general: Elena Azpiazu Garrido**

Se encarga de dar soporte y apoyo al funcionamiento de las diferentes unidades de la Agencia, de elaborar informes y propuestas y de la secretaría del Consejo Consultivo.

5. **Registro general de protección de datos**

**Subdirector general del Registro General de Protección de datos: Julián Prieto Hergueta**

Se encarga de:

- Velar por la publicidad de los tratamientos de datos.
- Inscribir los ficheros de los que sean titulares las Administraciones públicas y los de titularidad privada.
- Las autorizaciones de transferencias internacionales de datos y los códigos de conducta.
- La autorización de datos para fines históricos, estadísticos o científicos.

# 2- Registro de ficheros

## *2.1 – Definiciones básicas*

La **Ley Orgánica de Protección de Datos (LOPD)** establece las obligaciones que los responsables de los ficheros han de cumplir para garantizar el derecho a la protección de datos de carácter personal.

La LOPD define al **responsable del fichero o tratamiento** como la "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no la realice materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados*.

La Ley Orgánica de Protección de Datos entiende por **fichero** a "*todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"*.

Por otro lado, entiende por **tratamiento** "*cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, asó como las cesiones de datos que resulten de comunicaciones, consultas interconexiones y transferencias"*.

(Las **definiciones de fichero y tratamiento** se encuentran en los **artículos 51.k y 51.t** respectivamente del **RLOPD**).

## *2.2 – Ficheros sometidos a inscripción y proceso de registro*

Siempre que se proceda al tratamiento de datos personales que suponga la inclusión de dichos datos en un fichero, el fichero se encontrará sometido a la Ley, **siendo obligatoria su inscripción** en el Registro General de Protección de Datos (RGPD).

Todo fichero de datos de carácter personal de titularidad pública o privada, con excepción de algunos ficheros excluidos en el artículo 2.2 de la LOPD, serán notificados a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos. No solicitar la inscripción constituye una infracción leve, además, la inscripción de ficheros debe estar actualizada en todo momento.

Para inscribir, suprimir o modificar la inscripción de un fichero en el Registro General de Protección de Datos, se deberá cumplimentar el modelo establecido de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán

efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos.
**Son objeto de inscripción en el Registro General de Protección de Datos:**

- Los ficheros de Administraciones Públicas.
- Los ficheros de titularidad privada.
- Las autorizaciones de transferencias internacionales de datos de carácter personal con destino a países con un nivel de protección semejante al de la LOPD.
- Los códigos tipo referenciados en el artículo 32 de la LOPD.
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

El Servicio Electrónico NOTA permite la presentación de notificaciones a través de Internet, también se puede presentar en papel. Dicho servicio se encuentra disponible en la Sede Electrónica de la Agencia Española de protección de datos.

## *2.3 – El sistema NOTA*

El **sistema de Notificaciones Telemáticas a la AEPD (NOTA)** permite a los responsables de ficheros con datos de carácter personal de titularidad pública y de titularidad privada:

- Cumplir con la obligación de notificar sus ficheros a la AEPD a través de una herramienta que informa y asesora acerca de los requerimientos de la notificación.
- Presentar de forma gratuita de notificaciones a través de Internet con certificado de firma electrónica. En caso de no disponer de un certificado de firma electrónica también puede presentar la notificación a través de Internet.
- Notificar de forma simplificada una serie de ficheros relacionados con distintas materias de titularidad pública y privada.
- Conocer el estado de tramitación de las notificaciones remitidas a través de Internet, mediante certificado de firma electrónica o mediante el código de envío generado por el formulario electrónico.
- Consultar el contenido completo de la inscripción de sus ficheros en la web de la Agencia.

## *2.4 – Formatos y especificaciones XML*

Además del sistema NOTA, la AEPD ha puesto en disposición de los responsables de ficheros un sistema de notificación basado en un formato estándar que permita el intercambio de información

entre diferentes plataformas **(formato XML)**. De esta forma tanto los responsables que desarrollen sus propios programas como aquellos que desarrollen paquetes ofimáticos de protección de datos pueden comunicarse con la AEPD para notificar sus ficheros.

Estos mensajes en formato XML pueden ser presentados con y sin certificado electrónico de firma reconocido.

En caso de que se presenten firmados electrónicamente:

- Deberán usar el estándar de firma XML.

- Una vez enviadas las notificaciones al Registro Telemático de la AEPD, este devolverá un mensaje confirmando la recepción del envío e incluyendo los datos necesarios para que el programa desarrollado por terceros configure el acuse de recibo de acuerdo con el formato establecido por la AEPD.

En caso de que las notificaciones se presenten mediante formato XML sin certificado de firma electrónica:

- El servidor web de la AEPD devolverá un mensaje confirmando la recepción del mensaje.

- El mensaje devuelto incluirá los datos necesarios para que el programa desarrollado por terceros configure la Hoja de solicitud de acuerdo con el formato establecido por la AEPD.

Para obtener los formatos y especificaciones XML de Titularidad Pública y formatos y especificaciones de Titularidad Privada se debe acceder a este enlace.

# 3- El documento de seguridad

## *3.1 – ¿Qué es el documento de seguridad?*

El documento de seguridad es el documento que deben tener todas las empresas y profesionales que deben cumplir con la Ley Orgánica de protección de Datos.

Las empresas que deben cumplir con la LOPD son todas aquellas que recojan datos personales de personas físicas y, en ese sentido, **el documento de seguridad debe recoger las medidas de seguridad de la empresa respecto a los datos personales que trata.**

Siempre que recojamos y tratemos datos personales de personas físicas estaremos obligados a cumplir con la LOPD y, por lo tanto, **estaremos obligados a tener un documento de seguridad.**

## *3.2 – Artículo 9 de la Ley Orgánica 15/1999*

El artículo 9 de la Ley Orgánica 15/1999 del 13 de diciembre de Protección de Datos de Carácter Personal establece en su punto 1 que "*el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".*

## *3.3 – Artículo 88.1 del Real Decreto 1720/2007*

El artículo 88.1 del Real Decreto 1720/2007 del 21 de diciembre establece la necesidad de disponer de un documento de seguridad:

*"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."*

## *3.4 – ¿Qué debe contener el documento de seguridad?*

El documento de seguridad contendrá:

1. **Identificación de la empresa, sus servicios y ámbito de aplicación** del documento de seguridad.

2. **Los ficheros** que la empresa tiene (clientes, pacientes, trabajadores, etc.) y su estructura, es decir, nombre del fichero, origen de los datos, forma de tratamiento de los datos (soporte

papel o informático), tipos de datos que se recogen, nivel de seguridad del fichero y la empresa encargada de gestionar el fichero si la hubiera.

3. Cuales son las **medidas de seguridad** que las empresas tienen para proteger esos ficheros, señalar, entre otras: armarios cerrados con llave, destructoras de papel, contraseñas personales en los ordenadores con acceso a datos personales, caducidad de las contraseñas, etc.

4. Relación de los **encargados del tratamiento**, es decir, de las empresas que se ha contratado la prestación de un servicio y en función de dicha prestación tienen accesos a datos personales. Por ejemplo, la gestoría laboral, gestoría fiscal, la empresa de mantenimiento informático, la empresa de prevención de riesgos laborales, etc.

5. **Inventario** de: los soportes con acceso a datos personales dónde se realizan las copias de seguridad, de los equipos informáticos que tienen acceso a datos y de los programas informáticos.

6. **Lista del personal de la empresa con acceso a datos** y las funciones de cada uno de ellos (a qué ficheros acceden y a qué pueden acceder con los datos personales que tratan).

En este sentido el artículo 88.3 del RLOPD establece lo siguiente:

"*El documento deberá contener, como mínimo, los siguientes aspectos:*

*A. Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.*

*B. Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.*

*C. Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.*

*D. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.*

*E. Procedimiento de notificación, gestión y respuesta ante las incidencias.*

*F. Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.*

*G. Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos."*

Por otra parte, el apartado 4 del artículo 88 añade lo siguiente:

*"En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:*

A. *La identificación del responsable o responsables de seguridad.*

B. *Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento."*

## *3.5 – Actualización del documento de seguridad*

El documento de seguridad debe mantenerse actualizado, ya que el artículo 88.7 establece lo siguiente:

*"El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas."*

Por lo tanto el documento de seguridad deberá actualizarse siempre que haya cambios sustanciales y, en su caso, anualmente para mantenerlo en todo momento actualizado, según la situación de la empresa.

## *3.6 – Consecuencias de no disponer de un documento de seguridad*

La principal consecuencia de no disponer de documento de seguridad es la imposición de una sanción por parte de la Agencia Española de Protección de Datos. En este caso en particular, podría tratarse de una sanción grave por no cumplir con las medidas de seguridad del RLOPD y podría alcanzar un coste de 300.000 euros.

Además, debemos tener en cuenta que en caso de recibir una denuncia por vulneración del derecho a la protección de datos, la AEPD tendrá en cuenta a la hora de cuantificar la sanción si cumplimos o no con la normativa y si, entre otras cosas, disponemos de documento de seguridad.

## *3.7 – Modelo del documento de seguridad*

La Agencia Española de Protección de Datos ha puesto en su página web una guía para elaborar el documento de seguridad y un modelo de seguridad editable, dicho modelo es accesible a través del siguiente enlace:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.pdf

El modelo consta de las siguientes partes:

1. **Ámbito de aplicación del documento.**

En este apartado se incluye el nombre del responsable del fichero. Así como una lista de los ficheros con su tipo de tratamiento (manual, automático o mixto) y su nivel de seguridad (bajo, medio, alto).

2. **Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.**

En este punto se especifican todas las opciones de restricción de acceso a los ficheros y el control de las mismas. Además se indica dónde se guardarán los datos físicamente y bajo qué medidas de seguridad, así como el control de las copias temporales y de recuperación.

3. **Información y obligaciones del personal.**

Aquí se especifica las obligaciones del personal de mantener un total secretismo sobre los datos que manejan y los métodos que se emplean para mantener al personal informado de sus obligaciones. También se informa de las consecuencias del inclumplimiento de lo especificado en el documento de seguridad.

4. **Procedimientos de notificación, gestión y respuesta ante las incidencias.**

En esta parte se redactará el procedimiento a llevar a cabo al detectar una incidencia. Se incluirán a quien hay que avisar de la incidencia, quien se encargará de corregirla y qué métodos se usará para ello.

5. **Procedimientos de revisión.**

El documento de seguridad se actualizará siempre que se produzca un cambio relevante en el sistema, en el contenido del fichero o en consecuencia de los controles periódicos. En este punto se indican los procedimientos que se tienen que llevar a cabo para mantener el documento de seguridad siempre actualizado.

**Anexo I - Descripción de ficheros.**

En el anexo se incluirá una lista de los ficheros, el personal que tiene acceso al mismo y su identificación en el RGPD. También se incluye la información sobre qué tipo de datos contiene, sus posibles usos, cesiones, etc.

**Anexo II - Nombremientos.**

Se especifica una lista con los cargos temporales que el responsable del fichero haya asignado.

**Anexo III - Autorizaciones de salida o recuperación de datos.**

Se incluyen las autorizaciones que el responsable del fichero ha otorgado para la salida de soportes que contengan una copia del fichero, aunque esta sea solo temporal. También se incluyen las

autorizaciones para la realización de procedimientos de recuperación de datos.

**Anexo IV - Delegación de autorizaciones.**

Presenta una lista de las personas a las que el responsable del fichero delega las autorizaciones en caso de no poder otorgarlas él mismo.

**Anexo V - Inventario de soportes.**

Indica los soportes que contienen la información que se incluye en el fichero, se indica que tipo de información contiene y donde se almacena.

**Anexo VI - Registro de incidencias.**

Se amplía la información respecto a las incidencias específicas en el apartado 3 del documento de seguridad.

**Anexo VII - Encargados de tratamiento.**

Copia del contrato que firmará el encargado del tratamiento del fichero, el cual estipula que los datos se tratarán de acuerdo a las especificaciones del responsable del fichero y nunca con un fin distinto al especificado en dicho contrato.

**Anexo VIII - Registro de entrada y salida de soportes.**

En este apartado se incluye un registro de los diferentes soportes de almacenamiento en los que figuran los datos especificados en el documento.

**Anexo IX - Medidas altenativas.**

Se indican las medidas alternativas para llevar el control de los dispositivos de almacenamiento que contienen los ficheros que no pueden registrarse y llevar un control respecto a lo indicado en la RLOPD.

# 4- El personal involucrado

A continuación vamos a analizar el papel de los diferentes personajes que aparecen el la Ley Orgánica de Protección de Datos 15/1999. Dichos personajes son los siguientes: **responsable del fichero, afectado o interesado, encargado del tratamiento, usuario y responsable de seguridad.**

## *4.1 – Responsable del fichero*

La Ley Orgánica de Protección de Datos se refiere con "**responsable del fichero**" a la persona, empresa o entidad responsable de que los datos de carácter personal almacenados en un fichero sean tratados aplicando las garantías que la propia LOPD establece para proteger la intimidad y demás derechos fundamentales de las personas.

Generalmente, aquella persona o entidad que en el ejercicio de su actividad decida crear un fichero para tratar los datos de las personas con las que se relaciona (clientes, proveedores, empleados, etc.) adquiere la condición de responsable del fichero y asume la obligación de tratar los datos aplicando las garantías previstas en la LOPD.

La definición que da el artículo 3.d de la LOPD el responsable del fichero es aquella "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente".*

**Obligaciones:**

El responsable del fichero debe poner todos los medios que sean necesarios para que los datos de carácter personal se utilicen aplicando las garantías que la Ley Orgánica de Protección de Datos establece para garantizar la intimidad y demás derechos fundamentales de los ciudadanos. Podemos resumir dichas obligaciones de la siguiente manera:

- **Notifición e inscripción de ficheros.** Cuando el responsable del fichero vaya a crear un fichero de datos de carácter personal debe notificarlo previamente a la Agencia Española de Protección de Datos con la finalidad de que, su cumple con los requisitos legalmente establecidos, sea inscrito en el Registro General de Protección de Datos.

- **Aplicación de los principio de la Protección de datos.** El responsable del fichero debe recoger, tratar y ceder los datos de carácter personal aplicando todos y cada uno de los principios regulados, los cuales son los siguientes: calidad de los datos, derecho de información en la recogida de datos, consentimiento del afectado, datos especialmente protegidos, seguridad de los datos, deber de secreto, comunicación de datos y acceso a los datos por cuenta de terceros.

- **Ejercicio de los derechos de los ciudadanos.** El responsable del fichero deberá diseñar y poner en marcha un procedimiento sencillo y gratuito que facilite a los ciudadanos el ejercicio de los denominados "derechos ARCO" (acceso, rectificación, cancelación y oposición).
- **Transferencia internacional de datos.** El responsable del fichero no podrá transmitir los

datos de carácter fuera del territorio del Espacio Económico Europeo salvo que el Director de la Agencia Española de Protección de Datos se lo haya autorizado previamente, debiendo tener en cuenta que no será necesaria dicha autorización cuando la transferencia tenga como objeto alguna de las excepciones previstas en el artículo 34 de la LOPD.

- **Colaboración con la Agencia.** El responsable del fichero tiene el deber de colaborar con la AEPD en el ejercicio de sus funciones, facilitando la función inspectora, proporcionando la información requerida y remitiendo las notificaciones legalmente previstas.

En caso de que el tratamiento de los datos de carácter personal no cumpla con las garantías previstas en la LOPD, el responsable del fichero se expone a ser sancionado con **multas de hasta 600.000 euros** en función del tipo de infracción que haya cometido.

## *4.2 – Afectado o interesado*

Se define al afectado o interesado como aquella persona física, titular de los datos que sean objeto del tratamiento.

Se define el tratamiento de datos como operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

## *4.3 – Encargado del tratamiento*

El término "**encargado del tratamiento**" hace referencia a la persona o entidad que accede a los datos de carácter personal para prestar algún tipo de servicio al responsable del fichero. Esta figura se define legalmente como "*la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio*".

El régimen jurídico aplicable a la figura de encargado del tratamiento se encuentra regulado en el **artículo 12 de la Ley Orgánica 15/1999** y en los **artículos 20 a 22 del Real Decreto 1720/2007.**

**Contrato de prestación de servicios:**

El acceso a los datos por parte del encargado del tratamiento y su posterior tratamiento por cuenta del responsable del fichero se denomina jurídicamente "**acceso a los datos por cuenta de terceros**" y para que sea legalmente válido debe estar fundamentado en la **prestación de un servicio** y debe estar regulado en un **contrato que deberá constar por escrito** o en alguna forma que permita acreditar su celebración y contenido.

Tal y como establece el artículo 12 de la LOPD, el contrato de "acceso a los datos por cuenta de terceros" debe establecer expresamente los siguientes extremos:

- **Tratamiento de los datos.** El encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.

- **Finalidad del tratamiento**. En el contrato quedará reflejada la finalidad con la que se deben tratar los datos, y el encargado del tratamiento obligará a no utilizar los datos con otros fines.

- **Comunicación de datos.** El encargado del tratamiento no comunicará los datos, ni siquiera para su conservación, a otras personas.

- **Medidas de seguridad.** En el contrato se estipularán, asimismo, las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

- **Finalización del servicio.** Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

- **Consecuencias del inclumpimiento del contrato.** Si el encargado del tratamiento destina los datos a otra finalidad, los comunica o los utiliza incumpliendo las estipulaciones del contrato, será también considerado responsable del tratamiento, respondiendo a las infracciones en que hubiera incurrido personalmente.

Cabe mencionar que, como establece el artículo 21 del RLOPD **el encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento** que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido autorización por parte del responsable del tratamiento para ello.

Como hemos dicho antes, **si el encargado del tratamiento incumple las condiciones del contrato será considerado responsable del tratamiento**, por lo que también podría enfrentarse a multas de hasta 600.000 euros.

## *4.4 – Usuario*

Este es el personaje más simple de la LOPD, ya que nos referimos al usuario como sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

## *4.5 – Responsable de seguridad*

Persona o personas de la organización a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Cuando se trate de ficheros de nivel medio o alto, el responsable del fichero deberá designar uno o

varios responsables de seguridad, encargados de coordinar y controlar las medidas definidas de seguridad, encargados de coordinar y controlar las medidas definidas de seguridad recogidas en el Documento de Seguridad, elaborado por el responsable del fichero. Este documento será de obligado cumplimiento para el personal con acceso a los sistemas de información y deberá contener una serie de aspectos mínimos referentes al ámbito de actuación, los procedimientos, la estructura de los ficheros y el tratamiento de los datos, entre otros temas.

El artículo 95 nos habla sobre el responsable de seguridad:

"*En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciado según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.*

*En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.*"

Entre las funciones del responsable de seguridad destacan la de analizar los informes de auditoría y elevar al responsable del fichero las recomendaciones y medidas correctoras oportunas, mantener el control de los registros de acceso, revisión de los registros de incidencias, y actualización del documento de seguridad.

# 5- Control de accesos

## *5.1 – ¿Qué es el control de accesos?*

La definición más generalizada de un **sistema de control de acceso** hace referencia al mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos, es decir, es un mecanismo a través del cual puedes acceder a ciertos lugares físicos o datos lógicos únicamente si te has identificado previamente y además esa identificación ha sido autentificada. Básicamente encontramos sistemas de controles de acceso en múltiples formas y para diversas aplicaciones. Por ejemplo, encontramos sistemas de controles de acceso por software cuando digitamos nuestra contraseña para abrir el correo.

Resumiendo el **control de acceso** consiste en la verificación de si una entidad solicitando acceso a un recurso tiene los **derechos necesarios para acceder.** Un control de acceso ofrece la posibilidad de acceder a recursos físicos o **lógicos** (como por ejemplo, una aplicación informática o un **archivo**).

## *5.2 – ¿Para que se usa?*

Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos (ej: acceso a una habitación donde hay servidores), recursos lógicos (ej: una cuenta de banco, de donde solo determinadas personas pueden extraer dinero) o recursos digitales (ej: un archivo informático que sólo puede ser leído, pero no modificado).

## *5.3 – ¿De que esta compuesto?*

El control de acceso esta formado por tres componentes:

- Un **mecanismo de autenticación de la entidad** (como una contraseña o una clave),
- Un **mecanismo de autorización.**
- Un **mecanismo de trazabilidad,** dotando de responsabilidad a las entidades y permitiendo identificar al responsable de una acción.

Cada uno de estos 3 componentes tienen una función independiente.

## *5.4 – Que tipos hay y que pasos los componen.*

**TIPOS DE CONTROL DE ACCESOS**

- Gestión de accesos de usuario
  - Gestión de accesos de usuario Registro de usuarios
  - Gestión de privilegios
  - Gestión de contraseñas de usuario
  - Revisión de los derechos de acceso de los usuarios

- Control de accesos al sistema operativo
  - Control de accesos al sistema operativo
  - Procedimientos de conexión de terminales
  - Identificación y autenticación de los usuarios
  - Sistema de gestión de contraseñas Utilización de utilidades del sistema
  - Timeout de sesiones
  - Limitación del tiempo de conexión

- Control de acceso a la información y aplicaciones
  - Control de acceso a la información y aplicaciones
  - Restricción de acceso a la información Aislamiento de sistemas sensibles

- Control de accesos en red
  - Control de accesos en red
  - Política de uso de los servicios de red
  - Autenticación para conexiones externas
  - Identificación de equipos en la red
  - Protección a puertos de diagnóstico remoto y configuración
  - Segregación en las redes
  - Control de conexión a las redes
  - Control de enrutamiento en red

El concepto de control de acceso **consta de tres pasos**:

Estos pasos son la **identificación, autenticación y autorización**. Con el uso de estos tres principios un administrador o un Controlador automatizado del sistema pueden controlar qué recursos están disponibles para los usuarios del mismo.

- **La identificación** se refiere al proceso de Validar quien es el Usuario del sistema. Es el medio por el cual un usuario se identifica.

- **La autenticación** es el segundo paso del proceso de control de acceso. Contraseñas, reconocimiento de voz, y escáneres biométricos son métodos comunes de autenticación. El objetivo de la autenticación es para verificar la identidad del usuario del sistema.

- **La autorización** se produce después de que un usuario del sistema se autentica y luego es

autorizado a acceder. El usuario está generalmente **sólo autorizado a acceder ciertas áreas o zonas de los recursos del sistema en función de su papel en la organización.**

## *5.5 – Objetivos del control de acceso*

Los objetivos del control de acceso son los siguientes:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos. -Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

.

## *5.6 – Los niveles de seguridad*

Las medidas de seguridad previstas en el Real Decreto 1720/2007 se encuentran clasificadas en tres niveles (**básico, medio y alto**) que se aplicarán en función del tipo de datos que contenga el fichero y la finalidad del tratamiento de dichos datos.

Cuanto más sensibles sean los datos tratados o más comprometido sea el tratamiento realizado, mayor nivel de seguridad será necesario para el archivo.

Las medidas de seguridad previstas en el reglamento de LOPD se **aplican acumulativamente,** es decir, cuanto mayor sea el nivel de seguridad del archivo, más medidas de seguridad serán implementadas. Por ejemplo, a un fichero con un nivel de seguridad medio se le aplicarán también las medidas de seguridad de un fichero de nivel básico.

## *5.7 – ¿Qué es un fichero automatizado y un fichero no automatizado?*

**Ficheros automatizados:**

La normativa sobre protección de datos se refiere a los ficheros automatizados como *todo conjunto organizado de datos de carácter personal que permita acceder a la información relativa a una persona física determinada usando procedimientos de búsqueda automatizados*. Dentro de este concepto están incluidos los ficheros de datos personales que almacenan la información en **soportes informáticos**, como bases de datos, y que permiten acceder a los datos personales utilizando cualquier tipo de aplicación o procedimiento informatizado.

**Ficheros no automatizados**

Están definidos legalmente como *todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.* Un ejemplo de fichero no automatizado serían los archivadores existentes en la mayoría de de las organizaciones en los que se almacenan **expedientes de documentos.**

## *5.8 – Real Decreto 1720/2007*

En 2007 se aprobó el **Real Decreto 1720/2007**, donde se desarrolló la Ley Orgánica de Protección de Datos de Carácter Personal, tal como se refleja en el artículo 1:

"*El presente reglamento tiene por objeto el desarrollo de la* ***Ley Orgánica 15/1999 de 13 de diciembre,*** *de Protección de datos de carácter personal."*

En este Real Decreto, en los **artículos 91 y 92** se desarrolló las características del **control de accesos** y de **de gestión de soportes y documentos.**

## *5.9 – Medidas de seguridad para ficheros y tratamientos automatizados*

| | Medidas de seguridad | Nivel Basico | Nivel Medio | Nivel Alto |
|---|---|---|---|---|
| 1 | » Funciones y obligaciones del personal | Si | Si | Si |
| 2 | » Registro de incidencias | Si | Si | Si |
| 3 | » Control de acceso | Si | Si | Si |
| 4 | » Gestión de soportes y documentos | Si | Si | Si |
| 5 | » Identificación y autenticación | Si | Si | Si |
| 6 | » Copias de respaldo y recuperación | Si | Si | Si |
| 7 | » Responsable de seguridad | ------ | Si | Si |
| 8 | » Auditoria | ------ | Si | Si |
| 9 | » Gestión de soportes y documentos | ------ | Si | Si |
| 10 | » Identificación y autenticación | ------ | Si | Si |
| 11 | » Control de acceso físico | ------ | Si | Si |
| 12 | » Registro de incidencias | ------ | Si | Si |
| 13 | » Gestión y distribución de soportes | ------ | ------ | Si |
| 14 | » Copias de respaldo y recuperación | ------ | ------ | Si |
| 15 | » Registro de accesos | ------ | ------ | Si |
| 16 | » Telecomunicaciones | ------ | ------ | Si |

A continuación hablaremos de un gran número de artículos de interés pertenecientes al Real Decreto 1720/2007 de la LOPD.

**Para un nivel de seguridad básico:**

**Artículo 89 - Funciones y obligaciones del personal**

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

**Artículo 90 - Registro de incidencias (pero poco importante, de pasada)**

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

**Artículo 91 - Control de acceso**

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

**Artículo 93 - Identificación y autenticación**

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

**Para un nivel de seguridad medio:**

**Artículo 95 - Responsable de seguridad**

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

**Artículo 98 - Identificación y autenticación**

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

**Artículo 99 - Control de acceso físico**

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

**Artículo 100 - Registro de incidencias (lo mismo, de pasada, y si eso)**

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

**Para un nivel de seguridad alto:**

**Artículo 103 - Registro de accesos**

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

## *5.10 – Medidas de seguridad para ficheros y tratamientos no automatizados*

**Para un nivel de seguridad básico:**

**Artículo 107 - Dispositivos de almacenamiento**

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

**Medidas de seguridad de nivel medio:**

**Artículo 109 - Responsable de seguridad**

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

**Medidas de seguridad de nivel alto:**

**Artículo 113 - Acceso a la documentación**

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

## *5.11 – Tabla resumen*

| Nivel Básico | Nivel Medio | Nivel Alto |
|---|---|---|
| ✓ Los usuarios accederán únicamente a los datos y recursos necesarios para sus funciones.<br>✓ Habrá mecanismos para evitar el acceso con distintos derechos de los autorizados.<br>✓ La concesión de derechos de acceso sólo la dará personal autorizado. | ✓ Existirán controles de acceso físico a los locales donde se encuentren ubicados los sistemas de información. | ✓ Existirá un Registro de Accesos donde figurará:<br>✓ usuario,<br>✓ hora,<br>✓ fichero,<br>✓ tipo acceso<br>✓ registro accedido.<br>✓ Estará bajo el control del responsable de seguridad.<br>✓ Se hará un informe mensual.<br>✓ Se conservará al menos durante 2 años. |
| *Aplicable a ficheros automatizados y manuales* | *Aplicable solo a ficheros automatizados* | |

| Nivel Básico Nivel Medio | Nivel Alto |
|---|---|
| ✓ Los usuarios accederán únicamente a los datos y recursos necesarios para sus funciones.<br>✓ Habrá mecanismos para evitar el acceso con distintos derechos de los autorizados.<br>✓ La concesión de derechos de acceso sólo la dará personal autorizado. | ✓ El acceso se limitará al personal autorizado.<br>✓ Habrá mecanismos para identificar los accesos a documentos disponibles para múltiples usuarios<br>✓ Procedimiento en el Documento de Seguridad para registrar los accesos de otras personas |
| *Aplicable a ficheros automatizados y manuales* | *Aplicable solo a ficheros manuales* |

# 6- Gestión de soportes y documentos

## *6.1 – Aclaraciones básicas*

La Ley Orgánica de Protección de Datos deja claro que los soportes y documentos que contengan datos de carácter personal deben permitir identificar el tipo de información que contienen, ser inventariados y solo deben ser accesibles por el personal autorizado para ello en el documento de seguridad.

Los soportes deberán permitir identificar el tipo de información, que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en este documento.

A continuación vamos a hablar de diferentes artículos relacionados con la gestión de soportes y documentos:

## *6.2 – Ficheros automatizados*

**Medidas de seguridad de nivel básico:**

**Artículo 92 - Gestión de soportes y documentos**

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

**Medidas de seguridad de nivel medio:**

**Artículo 97 - Gestión de soportes y documentos**

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de

envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

**Medidas de seguridad de nivel <u>alto:</u>**

**Artículo 101 - Gestión y distribución de soportes**

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

## *6.3 – Ficheros no automatizados*

**Artículo 106 - Criterios de archivo**

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

**Artículo 108 - Custodia de los soportes**

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

**Medidas de seguridad de nivel <u>alto:</u>**

**Artículo 111 - Almacenamiento de la información**

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté

protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

**Artículo 114 - Traslado de documentación**

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

## *6.4 – Tabla resumen*

| Nivel Básico | Nivel Medio | Nivel Alto |
|---|---|---|
| ✓ Debe identificarse el tipo de datos que contienen.<br>✓ Existirá un inventario de soportes<br>✓ Se almacenarán en un lugar con acceso restringido.<br>✓ Deberá autorizarse la salida de soportes. | ✓ Habrá un registro de entrada y salida de soportes.<br>✓ Se adoptarán medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. | ✓ Cuando sea necesario distribuir soportes, se hará cifrando los datos o mediante cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros. |
| *Aplicable a ficheros automatizados y manuales* | *Aplicable solo a ficheros automatizados* | |

| Nivel Básico | Nivel Medio | Nivel Alto |
|---|---|---|
| ✓ Se aplicarán criterios de archivo que permitan la conservación, localización y consulta<br>✓ Los dispositivos de almacenamiento tendrán mecanismos que obstaculicen su apertura<br>✓ Cuando la documentación no se encuentre archivada, su depositario deberá custodiarla e impedir accesos no autorizados | | ✓ El acceso a armarios, archivadores, etc. estará protegido mediante puertas con cerradura. Cuando no se acceda, permanecerán cerradas.<br>✓ Soluciones alternativas, motivadas en el Documento de Seguridad<br>✓ Siempre que se proceda al traslado físico de documentación, deberán adoptarse medidas para impedir su acceso o manipulación |
| *Aplicable solo a ficheros manuales* | | |

# 7- Copias de seguridad

## *7.1 – ¿Qué son las copias de seguridad?*

Una **copia de seguridad** o **backup** es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos, como recuperar archivos eliminados accidentalmente, infectados por un virus informático o incluso eliminados a consecuencia de una catástrofe natural.

El proceso de copia de seguridad se complementa con el proceso de **restauración de los datos**, que es la acción de leer y grabar en la ubicación original u otra alternativa los datos requeridos.

La pérdida de datos es muy común, el 66% de los usuarios de Internet han sufrido una seria pérdida de datos en algún momento.

Es necesario crear copias de seguridad para evitar problemas legales, problemas administrativos y pérdidas económicas.

## *7.2 – ¿Obligaciones de la LOPD en materia de copias de seguridad?*

La LOPD obliga a todas las organizaciones, empresas e instituciones a garantizar la seguridad de datos de carácter personal que tratan y almacenan en sus sistemas de información y clasifica estos datos en los tres niveles de seguridad (básico, medio y alto).

### Básico:

**Datos de carácter personal (nombres, direcciones de teléfono, etc.):**

Afecta a cualquier actividad, empresa, agrupación, etc.

Tienen la obligación de realizar una copia de seguridad al menos una vez a la semana y deben garantizar la restauración de datos al momento anterior de producirse la pérdida (artículo 94.1 del RLOPD 1720/2007).

### Medio:

**Datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, Servicios Financieros, solvencia patrimonial y crédito:**

Afecta especialmente a la Administración Pública, entidades financieras y sector público.

En este nivel de seguridad es necesaria una autorización para la ejecución de procedimientos de restauración de datos (artículo 100.2 del RLOPD 1720/2007).

## Alto:

**Datos relacionados con la ideología, origen racial, salud, creencias, afiliación sindical, religión y sexo**

Afecta especialmente a los centros de formación, partidos políticos, salud, RR.HH., clubs y agrupaciones de ocio y todas las empresas que gestionan sus nóminas .

Será necesario un almacenamiento externo de copias y procedimientos de restauración de datos (artículo 101 del RLOPD 1720/2007).

Es necesario recordar que **para cada nivel de seguridad también se deben cumplir de los niveles de seguridad inferiores** a este, es decir, en el nivel de seguridad alto se deben de cumplir las obligaciones de los niveles medio y básico y en el nivel medio se deben cumplir las obligaciones básicas.

## *7.3 – Artículos relacionados con las obligaciones de la LOPD*

**Artículo 101.2 - Cifrado de los datos**

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos garantizando que dicha información no sea vista ni manipulada durante su transporte.

Para la encriptación se recomienda un cifrado de 128 bits.

**Artículo 103 - Registro de accesos**

El administrador no tiene acceso a los datos salvo autorización expresa del cliente. En el caso de necesitar ejecutar una recuperación en el Data-Center, el usuario debe proporcionar su clave de seguridad. El acceso queda registrado.

**Artículo 102 - Copias de respaldo en un lugar diferente a aquél en que se encuentran los equipos informáticos que los tratan**

Es la funcionalidad principal de nuestras herramientas de Backup Online.

Obligatorio en las copias para la protección de datos de alto nivel.

**Artículo 104 - Transmisión de datos por redes de Telecomunicaciones**

Los datos se transmiten, cifrados y comprimidos, bajo protocolo de comunicación seguro SSL (https).

**Artículo 94.2 - Verificación periódica de la copia**

El responsable del fichero se encargará de verificar cada seis meses la correcta definición, aplicación y funcionamiento de los procedimientos de realización de copias de respaldo y recuperación de datos.

## *7.3 – Sanciones*

El incumplimiento de la Ley puede dar lugar a sanciones económicas, que en función de su gravedad pueden ser:

### LEVES:

No cumplir las instrucciones de la Agencia de Protección de Datos, poseer datos obsoletos, no rectificar o cancelar inexactitudes, etc. De **601 a 60.101 €.**

### GRAVES:

Crear ficheros con finalidades distintas al objeto legítimo de la entidad, tratar datos por parte de un centro sin la existencia de un contrato que recoja la problemática de la protección de datos, etc. De **60.101 a 300.506 €.**

### MUY GRAVES:

Comunicación o cesión no permitida de datos personales, vulneración de principios para datos especialmente protegidos. De **300.506 a 601.012 €.**

# 8- Seguimiento y control (Auditoría LOPD)

## *8.1 – ¿Qué es una auditoría de protección de datos?*

El artículo 96 del RLOPD afirma lo siguiente:

*"1 - 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.*

*2 - El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.*

*3 - Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas."*

Mediante la auditoría se verifica la correcta implantación de las medidas de seguridad a adoptar en la organización en función del nivel de seguridad que le corresponda (básico, medio y alto).

Una vez realizada la auditoría, **se elabora un informe** que registra los puntos verificados, salvedades detectadas y las medidas necesarias para su corrección. Este informe deberá ser analizado por el responsable de seguridad para hacer llegar al responsable del fichero todas las medidas correctoras pendientes de aplicar en la empresa.

El informe de auditoría es **obligatorio** para todas las empresas y organizaciones que tengan un **nivel de seguridad alto o medio** por el tipo de datos que almacenan.

Como dice **el artículo 96 del RLOPD**, también será necesario **cada dos años** realizar una auditoría salvo que se realicen cambios sustanciales en el tipo o tratamiento de los datos personales que impliquen un cambio de las medidas de seguridad necesarias.

## *8.2 – Objetivos de la auditoría*

Los objetivos que se persiguen al realizar una auditoría son los siguientes:

1. Satisfacer la obligación de verificar las medidas de seguridad cada 2 años.

2. Constatar **posibles deficiencias** en el sistema de información de la empresa, y establecer acciones correctoras.

3. Considerar **oportunidades de mejora** y recomendaciones sobre las propias medidas de seguridad auditadas, en un proceso de mejora continua.

4. Estudiar en detalle flujos de datos personales o procedimientos internos en los que la LOPD tiene un especial impacto, para ajustarlos a la normativa.

5. **Concienciar y preparar** al personal sobre la importancia de la información personal, asegurando de esta forma la protección y los derechos de los afectados.

## *8.3 – ¿Qué puede hacer la auditoría?*

La propia Ley de Protección de Datos indica que la auditoría se puede realizar de manera **interna o externa,** esto quiere decir que se puede realizar **por la propia organización auditada o por una empresa externa.**

El profesional encargado de realizar la auditoría deberá estar especializado en este campo, debidamente capacitado en materia de protección de datos y con la característica de ser independiente, es decir, no tener ningún interés personal en la entidad.

El reglamento no obliga a realizar una auditoría en menos de dos años salvo modificaciones sustanciales, no obstante, es natural que en ese período de tiempo se produzcan cambios significativos en la empresa, por lo que es muy recomendable realizar una auditoría al menos anualmente.

## *8.4 – Pasos a seguir en un auditoría*

A la hora de realizar una auditoría de Protección de Datos debemos seguir una serie de pasos:

- **Revisar los documentos de la empresa:** debemos comprobar que se hayan firmado todos los contratos necesarios en materia de protección de datos. También tendremos que revisar si se han realizado modificaciones en el documento de seguridad o si se ha actualizado.

- **Revisar el sistema informático de la empresa:** habrá que comprobar si tenemos un sistema para asignar nuevos usuarios con contraseñas individualizadas, si las contraseñas caducan como mínimo una vez al año. Igualmente se deberá revisar si se realizan copias de seguridad, en qué formato y con qué periodicidad.
- **Revisar las instalaciones de nuestra empresa:** habrá que comprobar si disponemos de

sistemas seguros de destrucción de la información y si el acceso a archivos con datos personales, a las copias de seguridad o al servidor está limitado de algún modo.

- **Entrevistar a los responsables** de los departamentos de la empresa que puedan tener acceso a los datos personales para detectar si los circuitos de tratamiento de datos son acordes a lo que establece la normativa.

Una vez revisados todos estos puntos, el responsable de la auditoría deberá emitir un informe detallando los errores que la empresa debe corregir y las recomendaciones para mejorar. La empresa deberá corregir los errores marcados por el auditor y garantizar que los datos personales son tratados cumpliendo estrictos controles de seguridad y privacidad.

El informe no se envía a la AEPD, si no que se conserva como documento interno y se deberá poner a disposición de la AEPD si ésta lo solicita.

## *8.5 – Sanciones*

Según la LOPD, el incumplimiento del deber de seguridad será considerado como infracción grave con una sanción de 40.001 a 300.000 €.

Las medidas a adoptar para cumplir el deber de seguridad son una obligación de resultado ya que deben implantarse para evitar cualquier pérdida, alteración o acceso no autorizado a datos de carácter personal. Por tanto, el deber de seguridad no consiste en la obligación de implantar unas medidas sino en implantar esas medidas con un resultado concreto.

Podemos concluir, por tanto, que el hecho de no realizar la auditoría no es sancionable por sí mismo. Lo que se sanciona es la pérdida, alteración, acceso o tratamiento no autorizado de datos personales. Sin embargo, sí es recomendable realizar esa auditoría para asegurarnos de que disponemos de las medidas de seguridad adecuadas para evitar que se produzca ese resultado.

# Referencias:

## *Punto 1 - La agencia de protección de datos:*


http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/index-ides-idphp.php

http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/funciones-ides-idphp.php

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/CartaServiciosAEPD.pdf

https://www.urjc.es/images/proteccion_datos/B.4-cp--Directiva-95-46-CE.pdf

http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2


## *Punto 2 - Registro de ficheros:*


https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/index-ides-idphp.php

https://www.agpd.es/portalwebAGPD/canalresponsable/index-ides-idphp.php

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/index-ides-idphp.php

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/intercambios_masivos/index-ides-idphp.php

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/que_es/index-ides-idphp.php

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Desarrolladores_XML/index-ides-idphp.php


## *Punto 3 - El documento de seguridad:*


https://www.agpd.es/portalwebAGPD/canalresponsable/guia_documento/index-ides-idphp.php

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.pdf

http://evamunoz.es/que-es-documento-de-seguridad-lopd-contenido-modelo/

http://slideplayer.es/slide/1734583/

http://cuidatusdatos.com/obligacioneslopd/medidasseguridad/documentoseguridad/index.html

### *Punto 4 - El personal involucrado:*

http://www.iee.es/pages/bases/articulos/derint023.html

http://www.cuidatusdatos.com/infoencargado.html

http://www.cuidatusdatos.com/inforesponsable.html

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php

### *Punto 5 - Contro de accesos:*

http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.t8.html

http://cuidatusdatos.com/obligacioneslopd/medidasseguridad/automatizados/medidasautomatizados.html

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.pdf

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

http://www.grespro.com/productos/lista_politica-de-proteccion-de-datos_1.html

http://cuidatusdatos.com/obligacioneslopd/medidasseguridad/automatizados/index.html

http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.html

http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html

https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

https://es.wikipedia.org/wiki/Control_de_acceso#cite_note-KimSolomon-1

ttp://www.protegetuinformacion.com/docs/7/autonomos_2_lopd.pdf

http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.t8.html

http://www.cuidatusdatos.com/infofichero.html

http://boe.es/diario_boe/txt.php?id=BOE-A-2008-979

http://cuidatusdatos.com/obligacioneslopd/medidasseguridad/automatizados/medidasautomatizados.html

http://911alarmas.com/index.php?modulo=contenido&id=76

http://www.monografias.com/trabajos102/administracion-del-control-accesos-adecuado-sistemas-informacion/administracion-del-control-accesos-adecuado-sistemas-informacion.shtml

### *Punto 6 - Gestión de soportes y documentos:*

http://www.euskadi.eus/contenidos/normativa/medidas_seg_2007/es_1720/adjuntos/medidas_seguridad_RD-LOPD.pdf

http://www.euskadi.eus/contenidos/normativa/medidas_seg_2007/es_1720/adjuntos/medidas_seguridad_RD-LOPD.pdf

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

### *Punto 7 - Copias de seguridad:*

https://es.wikipedia.org/wiki/Copia_de_seguridad

http://www.gadae.com/blog/como-deben-hacerse-las-copias-de-seguridad-segun-la-lopd/

http://www.zarainfo.com/archivos/BackupOnline_3_LOPD.pdf

### *Punto 8 - Seguimiento y control (Auditoría LOPD):*

https://www.pymesyautonomos.com/tecnologia/guias-practicas-de-la-lopd-viii-la-auditoria-en-proteccion-de-datos

http://zugastiabogados.es/cuando-y-como-hay-que-realizar-una-auditoria-en-lopd/

http://ayudaleyprotecciondatos.es/2016/08/05/obligatoria-auditoria-proteccion-datos/