

# **Tema 7: Ley Orgánica de Protección de Datos**

**Grupo**  
**The Red Chicken**

Juan Francisco Bustos Correas  
Pablo Serna Martínez  
Yolanda Torregrosa Hernández  
Alejandro Torres Mateu  
Raquel Yuste Torregrosa



## Tabla de contenido

---

1.	La agencia de protección de datos.....	4
1.1.	¿Qué es la Agencia de Protección de Datos? .....	4
1.2.	Régimen Jurídico de la Agencia.....	4
1.3.	Organización y estructura de la Agencia.....	4
1.4.	Funciones de la Agencia de Protección de Datos.....	6
2.	Registro de ficheros.....	6
2.1.	¿Qué es el registro de ficheros? .....	6
2.2.	Ficheros a registrar .....	6
2.3.	¿Cómo inscribir ficheros? .....	7
2.4.	¿Cómo consultar ficheros? .....	7
2.4.1.	Búsqueda de ficheros de titularidad privada .....	8
2.4.2.	Búsqueda de ficheros de titularidad pública.....	8
2.4.3.	Búsqueda a través de árbol (Índice Organismos):.....	8
2.4.4.	Búsqueda a través de formulario (Búsqueda General): .....	9
3.	El documento de seguridad.....	10
3.1.	¿Qué es el Documento de Seguridad? .....	10
3.2.	¿Es obligatorio tener un documento de seguridad? .....	10
3.3.	¿Qué debe contener el Documento de Seguridad? .....	10
3.3.1.	Secciones del Documento de Seguridad .....	10
3.3.2.	Anexos del Documento de Seguridad .....	12
3.4.	Consecuencias de no disponer del Documento de Seguridad .....	14
3.5.	¿Debe actualizarse el documento de seguridad? .....	14
3.6.	¿Es obligatorio que los empleados conozcan la existencia y contenido del documento de seguridad? .....	15
4.	El personal involucrado .....	15
4.1.	Responsable del fichero .....	15
4.2.	Personal encargado del tratamiento.....	16
4.3.	Ciudadano o personal interesado o afectado .....	16
5.	Control de accesos .....	16
5.1.	¿Qué es el control de acceso? .....	16
5.2.	Componentes .....	16
5.3.	Control de acceso para ficheros automatizados .....	17
5.4.	Control de acceso para ficheros manuales .....	18
6.	Gestión de soportes y documentos .....	18
6.1.	Gestión de soportes para ficheros automatizados .....	18
6.2.	Gestión de soportes para ficheros no automatizados .....	20
7.	Copias de Seguridad .....	21

7.1.	¿Qué es una Copia de Seguridad? .....	21
7.2.	¿Por qué crear Copias de Seguridad?.....	21
7.3.	Almacenar Copias de Seguridad.....	22
7.4.	La Ley Orgánica de Protección de Datos y las Copias de Seguridad .....	22
7.5.	Estrategias de backup .....	24
7.6.	Plan de prevención genérico .....	24
7.6.1.	Cómo aplicarlo.....	24
7.6.2.	Cómo recuperar los archivos.....	24
7.7.	Conclusiones.....	24
8.	Seguimiento y control (Auditoría LOPD) .....	25
8.1.	¿Qué es una Auditoría de Protección de Datos? .....	25
8.2.	¿Quién debe realizar la auditoría? .....	25
8.3.	¿Cuáles son los pasos a seguir a la hora de realizar una auditoría? .....	25
8.4.	Informe de Auditoría .....	26

## 1. La agencia de protección de datos

---

### 1.1. ¿Qué es la Agencia de Protección de Datos?

---

La Agencia Española de Protección de Datos (AEPD) es el ente que se encarga de que las leyes acerca de la protección de los datos sean cumplidas y aplicadas, abarcando todo lo relativo a los derechos esenciales de todos los ciudadanos, como el derecho al acceso, la rectificación, la cancelación o la oposición. Es el órgano del estado con personalidad jurídica propia, totalmente independiente de las Administraciones Públicas, relacionado con el Gobierno a través del Ministerio de Justicia.

### 1.2. Régimen Jurídico de la Agencia

---

El sistema que establece y regula el funcionamiento de la Agencia Española de Protección de Datos se resumen en el Título VI de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal y en el Real Decreto 428/1993, del 26 de marzo, por el que se aprueba el Estatuto de la agencia.

### 1.3. Organización y estructura de la Agencia

---

La Agencia Española de Protección de Datos se estructura de la siguiente manera, en los siguientes cargos y departamentos:

#### *Director/a*

---

El Director/a es el mayor cargo de representación y dirección de la Agencia, sus actos se consideran como actos propios de la Agencia. Su nombramiento se realiza a través del Real Decreto de entre quienes compone el Consejo Consultivo y a propuesta del Ministro de justicia.

Su cargo dura cuatro años, a no ser que se realice una renuncia, un fallecimiento o una separación acordada por el Gobierno en caso de: incumplimiento grave de sus obligaciones; incapacidad sobrevenida para el ejercicio de su función; incompatibilidad o condena por un delito.

#### *Funciones de la Directora de la Agencia*

- Dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia y, como por ejemplo, resolver las inscripciones en el Registro General de Protección de Datos o autorizar la entrada en los locales en los que se hallen los ficheros, con el fin de proceder a las inspecciones pertinentes.
- La coordinación con las autoridades autonómicas.
- La representación de la Agencia en el ámbito internacional.
- Funciones de gestión, tales como adjudicar y formalizar los contratos y vigilar su cumplimiento y ejecución o aprobar gastos y ordenar pagos, dentro de los límites de los créditos del presupuesto de la Agencia.

### *El Consejo Consultivo*

Es un órgano que se encarga de asesorar a cerca de todo tipo de decisiones al Director/a y está compuesto por 10 miembros nombrados también por un periodo de 4 años.

Este se reúne cuando lo convoca el/la Director/a o al menos una vez cada seis meses y realiza informes en relación a las cuestiones que le plantea el/la Director/a o planteando propuestas propias en materia de protección de datos.

### *El Registro General de Protección de Datos*

El órgano encargado de velar por la publicación de la existencia de ficheros de datos personales, además de inscribir:

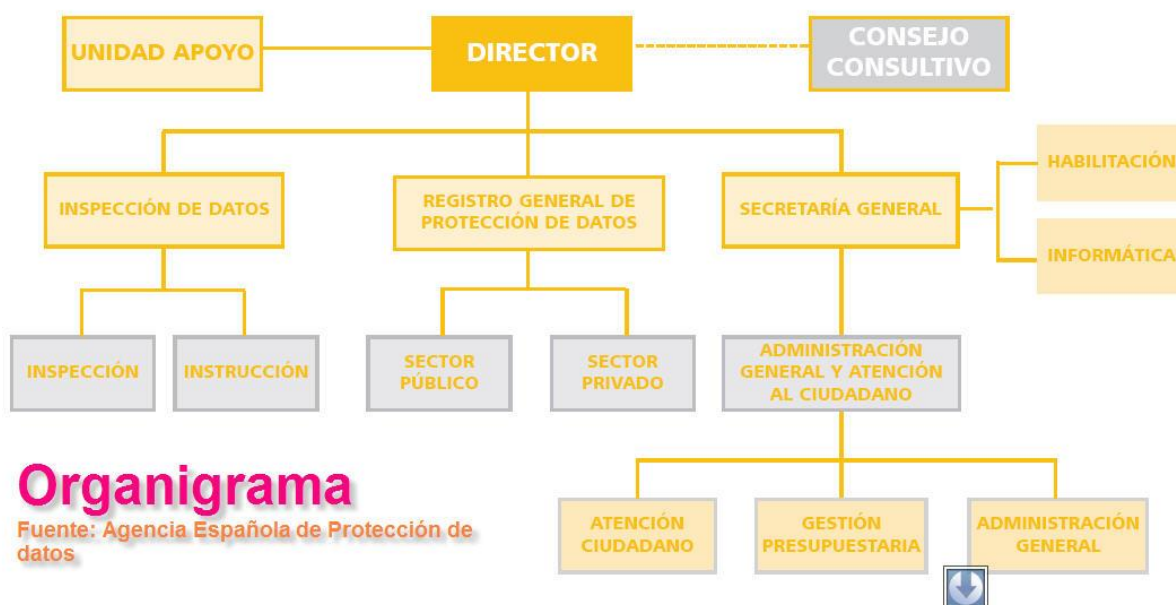
- los ficheros de los que sean titulares las Administraciones públicas o los organismos privados,
- las autorizaciones de transferencias internacionales de datos y códigos de conducta,
- y las autorizaciones de conservación de datos para fines históricos, estadísticos o científicos.

### *La Inspección de datos*

Tramita los procedimientos relativos al ejercicio de la potestad sancionadora que le atribuyen a la Agencia la LOPD, la LSSI y la LGT. Además, tutela los derechos de acceso, rectificación y oposición de los ciudadanos.

### *La Secretaría General*

La Secretaría General tiene tres funciones principales: asegurarse del correcto funcionamiento de los distintos órganos de la Agencia; elaborar informes y propuestas y ejercer de secretaría del Consejo Consultivo.



## 1.4. Funciones de la Agencia de Protección de Datos

Las funciones se establecen en el artículo 37 de la Ley Orgánica 15/1999 del 13 de diciembre de Protección de Datos de Carácter Personal, y son las siguientes:

Con los afectados	Con quienes tratan datos	En la elaboración de normas	En telecomunicaciones	Otras
Atender peticiones y reclamaciones	Emitir las autorizaciones	Informar los Proyectos de normas de la LOPD	Tutelar los derechos y garantías de los abonados y usuarios de las comunicaciones electrónicas	Cooperar con otros organismos internacionales
Informar de sus derechos	Requerir medidas de corrección	Informar los Proyectos de normas de protección de datos		Representar a España en la materia
Promover campañas de difusión	Ordenar los ceses y cancelaciones de datos	Dictar instrucciones para adecuar los tratamientos a la LOPD	Recibir notificaciones de las deficiencias de seguridad en los sistemas proveedores de servicios de comunicación	Control de lo relacionado con la ley reguladora de la Función Estadística Pública
Velar por la publicación de los ficheros personales	Ejercer la potestad sancionadora	Dictar recomendaciones de aplicación de leyes en materia de seguridad		Elaboración de una Memoria Anual

## 2. Registro de ficheros

### 2.1. ¿Qué es el registro de ficheros?

Cuando se disponga a almacenar datos de carácter personal de los usuarios de una aplicación es preciso que inscribamos los ficheros que contengan dicha información en el registro de la Agencia Española de Protección de Datos, como se especifica en el Artículo 26 de la Ley Orgánica de Protección de Datos.

La inscripción deberá estar siempre actualizada. Todo cambio que pueda afectar al contenido de la inscripción de los ficheros deberá ser notificado a la Agencia, así como la eliminación de esta inscripción. Si no realizamos la inscripción de los ficheros con datos de carácter personal esto constituirá una infracción leve.

### 2.2. Ficheros a registrar

Son objeto de inscripción en el Registro General de Protección de Datos:

- Los ficheros de las Administraciones Públicas
- Los ficheros de titularidad privada
- Las autorizaciones de *transferencias internacionales* de datos de carácter personal con destino a *países* que no presten un nivel de protección equiparable al que presta la LOPD a que se refiere el art. 33.1 de la citada Ley.

- Los códigos tipo, a que se refiere 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.

### 2.3. ¿Cómo inscribir ficheros?

Lo necesario para realizar la inscripción del fichero de carácter personal es rellenar el formulario que la Agencia Española de Protección de Datos pone en disposición de todos los usuarios en su Servicio Electrónico<sup>1</sup>, a través del cual deberá efectuarse la solicitud para el registro del fichero en el Registro General.

La presentación vía internet de notificaciones a través de este formulario con un certificado de firma electrónica es gratuita. En caso de que no se disponga de una firma electrónica, también será posible presentar notificaciones vía Internet, pero remitiendo a la Agencia la hoja de solicitud debidamente firmada.

Es posible también mediante dicho formulario notificar de forma simplificada acerca de los ficheros de titularidad privada. A través de esta opción se permite realizar los trámites que posteriormente podrán ser completados o adaptados a la situación actual del fichero que se está notificando.

Por último, se encuentran a libre disposición los diferentes formatos y especificaciones XML<sup>2</sup> que deben cumplir las los desarrolladores deseen implementar aplicaciones acerca de protección de datos para el envío de notificaciones a la AEP.

<sup>1</sup> Servicio Electrónico:

<https://sedeagpd.gob.es/sede-electronica-web/vistas/formNOTA/servicioNOTA.jsf>

<sup>2</sup> Especificaciones XML:

[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/intercambios_masivos/index-ides-idphp.php)

### 2.4. ¿Cómo consultar ficheros?

En la página web de la Agencia tenemos a nuestra disposición todos los ficheros inscritos en el Registro General de Protección de Datos. Estos son clasificados según la titularidad de sus responsables, es decir, podrán ser ficheros de titularidad privada o pública.

Dentro de los ficheros de titularidad pública se encontrarán los ficheros de los que sean responsables los siguientes entes u organismos:

- La **Administración Central** (Administración General del Estado, Entidades y Organismos de la Seguridad Social, Organismos Autónomos y Entes Públicos del Estado).
- La **Administración, Entes y Organismos Públicos de las Comunidades Autónomas**.
- La **Administración Local, Entes y Organismos Públicos de Entidades Locales**.
- **Otras Personas Jurídico Públicas**.

En titularidad privada aparecerán aquellos ficheros cuyo responsable sea una persona privada física o jurídica.



### 2.4.1. Búsqueda de ficheros de titularidad privada

---

Para consultar estos ficheros dispone de un formulario de búsqueda en el que se presenta una serie de campos de consulta. Introduzca en el/los campos correspondientes el texto por el que desea efectuar la consulta y presione el botón «Buscar» (si no se introduce ningún criterio se mostrará un mensaje para que especifique algún criterio de búsqueda).

Además, el formulario de búsqueda, presenta un campo denominado «Texto Libre». Si realiza la consulta a través de este campo, localizará todos aquellos ficheros que contengan el texto que haya introducido, en cualquiera de los campos del formulario de búsqueda.

Como resultado de la búsqueda obtendrá la relación de ficheros que cumplen los criterios establecidos, ordenados según la razón social y el nombre del fichero. La selección de uno de ellos da paso a una página en la que se detalla la información publicada para el fichero.

Para cada fichero inscrito en el Registro General de Protección de Datos se detallan, en una primera página de resumen, la siguiente información:

- Nombre o razón social del responsable del fichero
- Nombre del fichero
- Finalidad y usos declarados
- Dirección en la que el interesado puede ejercitar los derechos de oposición, acceso, rectificación y cancelación de la información contenida en el fichero

Desde esta página, se podrá mostrar información más detallada pulsando el botón **"Ver Más"**:

- Datos del responsable del fichero
- Derechos de oposición, acceso, rectificación y cancelación
- Identificación y finalidad del fichero
- Origen y procedencia de datos
- Tipos de datos, estructura y organización del fichero
- Cesión y comunicación de datos
- Transferencias internacionales

### 2.4.2. Búsqueda de ficheros de titularidad pública

---



En este apartado existen dos maneras de efectuar la consulta: a través de árbol (opción del menú "Índice Organismos") o a través de formulario (opción del menú "Búsqueda General").

### 2.4.3. Búsqueda a través de árbol (Índice Organismos):

---

El árbol reproduce la estructura jerárquica de los diferentes tipos de Administración, permitiendo navegar y desplegar sus ramas (Organismos, Centros Directivos y Unidades), hasta localizar el responsable buscado.

La pantalla se divide en dos partes, la superior contiene los criterios de selección utilizados hasta el momento y la inferior las posibles ramas accesibles desde ese punto.

-  Si aparece una carpeta se trata de una rama en la que puede profundizarse más.
-  Si se ha llegado a un documento ya está seleccionado un responsable.

#### 2.4.4. Búsqueda a través de formulario (Búsqueda General):

Para consultar estos ficheros dispone de un formulario de búsqueda en el que se presenta una serie de campos de consulta. Introduzca en el/los campos correspondientes el texto por el que desea efectuar la consulta y presione el botón «**Buscar**».

Además, el formulario de búsqueda, presenta un campo denominado «**Texto Libre**». Si realiza la consulta a través de este campo, localizará todos aquellos ficheros que contengan el texto que haya introducido, en cualquiera de los campos del formulario de búsqueda.

Como resultado de la búsqueda obtendrá la relación de ficheros que cumplen los criterios establecidos, ordenados según el encuadramiento administrativo del responsable y el nombre del fichero. La selección de uno de ellos da paso a una página en la que se detalla la información publicada para el fichero.

Para cada fichero inscrito en el Registro General de Protección de Datos se detallan, en una primera página, la siguiente información:

- **Tipo de Administración**, campo desplegable que permite seleccionar entre Administración Central, Autonómica, Local u Otras Personas Jurídico Públicas.
- **Comunidad Autónoma**, campo desplegable que permite seleccionar el nombre de la Comunidad (sólo válido para el caso de búsquedas de ficheros de Administración Autonómica).
- **Encuadramiento**, que se compone de tres apartados que identifican, en orden jerárquico, al responsable del fichero:
  - **Organismo**, nombre del Ministerio, Departamento o Entidad Local.
  - **Centro Directivo**, a nivel de Secretaría de Estado, Dirección General o asimilado.
  - **Unidad**, que identifica el elemento más específico dentro de esta estructura, como podría ser una Subdirección General o el equivalente dentro de cada tipo de Administración.
- Disposición de creación del fichero, que se compone de:
  - Tipo de Boletín.
  - Número de Boletín.
  - Fecha de Publicación del Boletín donde se encuentra publicada la disposición de carácter general que regula el fichero.
- Nombre del fichero.
- Finalidad y usos declarados.
- Dirección en la que el interesado puede ejercitar los derechos de acceso, rectificación y cancelación de la información contenida en el fichero.

Desde esta página, se podrá mostrar información más detallada pulsando el botón "Ver Más":

- Datos del responsable del fichero
- Derechos de oposición, acceso, rectificación y cancelación
- Diario Oficial, Número de Boletín y fecha de publicación de la disposición general de creación, modificación o supresión
- Identificación y finalidad el fichero
- Origen y procedencia de datos
- Tipos de datos, estructura y organización del fichero
- Cesión y comunicación de datos
- Transferencias internacionales.

### 3. El documento de seguridad

---

#### 3.1. ¿Qué es el Documento de Seguridad?

---

El documento de seguridad es un documento en el que se incluyen las normas, medidas de seguridad, procedimiento de actuación y tratamiento que deben cumplir los datos de nuestra empresa para garantizar la seguridad de estos. Esta seguridad será siempre acordada entre el responsable del fichero y el responsable de tratamiento de estos datos.

Este documento se encuentra regulado en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), concretamente en el Título 8, capítulo 2 artículo 88.

#### 3.2. ¿Es obligatorio tener un documento de seguridad?

---

Según la LOPD, estaremos obligados a disponer de un documento de seguridad siempre que tengamos a disposición y hagamos tratamiento de datos personales de personas físicas y reales. Por tanto, **sí es obligatorio disponer de un documento de seguridad**, siempre que tratemos con datos personales.

#### 3.3. ¿Qué debe contener el Documento de Seguridad?

---

El contenido debe quedar estructurado en cinco secciones y nueve anexos fijos y establecidos por la Agencia Española de Protección de Datos. A continuación vamos a tratar de qué contenido deberá incluir cada parte del documento.

##### 3.3.1. Secciones del Documento de Seguridad

---

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

---

Se deberá especificar cuál es la información y cuáles son los ficheros que la empresa posee en y su estructura, es decir, nombre del fichero, origen de los datos, si están en formato digital o en papel, tipos de datos que se recogen y nivel de seguridad del fichero. Además de esto ha de especificarse la empresa que se encarga de gestionar el fichero, si la hubiere.

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

---

Se deben especificar cuáles son las medidas de seguridad que se llevan a cabo en las empresas para garantizar la protección de los ficheros que contienen los datos. Estas pueden ser desde armarios o despachos cerrados con; contraseñas en los ordenadores con acceso a datos personales; cómo, dónde y cuándo se hacen las copias de seguridad; dónde se guardan las referidas copias de seguridad y con qué periodicidad se hacen.

- **Identificación y autenticación**

Medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales.

- **Control de acceso**

Se debe especificar que el personal de la empresa solo accederá a los datos que sea imprescindible acceder para poder desarrollar correctamente sus funciones en la empresa. Además se debe especificar los mecanismos que establecerá el responsable del fichero para evitar que un usuario pueda acceder a recursos que no esté autorizado a acceder, ya que sus derechos son distintos de los autorizados.

- **Registro de accesos**

En los accesos a los datos de los ficheros de nivel alto, se registrará por cada acceso 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. Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido.

Por lo tanto, en esta sección se deberá especificar información relativa al sistema de registros de acceso y el mecanismo que permitirá este registro bajo control directo del responsable de seguridad. Además se deberá especificar periodo de conservación de dichos accesos, que deberá ser al menos de dos años. No es preciso que estos datos se almacenen "on-line".

- **Gestión de soportes y documentos**

Se ha de indicar dónde y cómo se almacenan los soportes que contengan datos de carácter personal, lugar al que solo podrán acceder aquellas personas con autorización. Por lo tanto, se debe especificar también el listado de personas que tendrán acceso a estos soportes.

- **Acceso a datos a través de redes de comunicaciones**

Se ha de garantizar que las medidas de seguridad establecidas para acceder a los datos de carácter personal a través de redes de comunicación pueden otorgar un nivel de seguridad equivalente al que se garantiza al acceder a los datos en modo local. Además se ha de especificar en este punto los accesos que se prevé realizar y los ficheros que serán visualizados o manipulados en estos accesos.

- **Régimen de trabajo fuera de los locales de la ubicación del fichero**

Se debe especificar los ficheros que están autorizados a sufrir tratamientos fuera de los locales del responsable del fichero o mediante dispositivos portátiles, además de indicar cuáles son estos locales. Por último, también se ha de indicar cuál será el periodo de vigencia de la autorización para realizar estos tratamientos. Además, se deberá incluir el listado de usuarios que tendrán autorización para realizarlos, siempre garantizando el nivel de seguridad establecido para los datos tratados.

- **Traslado de documentación**

Se deberá especificar todas las medidas que será necesariamente que se lleven a cabo cuando sea preciso realizar un traslado físico de la documentación contenida en un fichero, siempre intentando garantizar que no se acceda o manipule la información durante este cambio de ubicación.

- **Ficheros temporales o copias de trabajo de documentos**

Se deberá especificar que los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda y serán borrados o destruidos una vez que hayan dejado de ser necesarios y carezcan ya de utilidad.

- **Copia o reproducción**

En este apartado debemos detallar los usuarios o perfiles de usuarios que estarán autorizados para realizar copias o reproducciones de documentos con datos personales. Además se deberá explicar los medios que se utilizarán para destruir las copias o reproducciones que finalmente se desechen, además de los usuarios que lo lleven a cabo.

- **Copias de respaldo y recuperación**

Especificaremos la periodicidad con la que se realizarán las copias de respaldo. En el Anexo I se detallarán los procedimientos de copia y recuperación para cada fichero.

- **Responsable de seguridad**

Por último se ha de especificar el responsable de seguridad que se encargará de coordinar y controlar las medidas que se definen en el Documento de Seguridad. La designación puede ser única para todos los ficheros o diferenciada según los sistemas de tratamiento, lo que se deberá especificar la parte correspondiente del Anexo I.

### *Información y obligaciones del personal*

---

En esta sección se especifica que el personal en conocimiento de los datos de carácter personal debe mantener un total secretismo sobre ellos. Además, se debe especificar cuáles son las funciones de éste personal ante los datos, es decir, cuáles son los métodos de acceso a los datos. Por último, también se deben especificar las consecuencias que supondrán el hecho de no cumplir lo especificado en el Documento de Seguridad.

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

---

Se habrá de especificar cuáles son los procedimientos que se llevarán a cabo cuando se detecte que se ha producido alguna incidencia, además de quiénes son los que habrá que avisar de que se ha producido dicha incidencia y quién será el encargado de corregirla y de cómo lo realizará.

### *Procedimientos de revisión*

---

Será preciso que se especifique cómo se ha de actuar ante la modificación del documento de seguridad, indicando siempre qué personas pueden proponer esos cambios y pueden aprobarlos después. A parte de esto, debe especificarse también qué personas se verán afectadas ante estos cambios para realizar las notificaciones pertinentes a estas.

Además, se ha de indicar los procedimientos para realizar la auditoría interna o externa que verifique el cumplimiento del Título VIII del RLOPD, referente a las medidas de seguridad. Por último, indicar también los procedimientos para realizar el informe mensual sobre el registro de accesos a los datos de nivel alto regulado por el artículo 103 del RLOPD.

## **3.3.2. Anexos del Documento de Seguridad**

---

### *Anexo I: Descripción de ficheros*

---

En este apartado se deberán de describir todos los ficheros que contengan datos personales y que necesiten se protegidos siguiendo la siguiente estructura:

- Nombre del fichero o tratamiento
- Unidad/es con acceso al fichero o tratamiento
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos

- ☐ Identificador
  - ☐ Nombre
  - ☐ Descripción
- Nivel de medidas de seguridad a adoptar
- Administrador
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento
- Código Tipo Aplicable (*si el fichero está incluido en el ámbito de alguno de los códigos tipo regulados por el artículo 32 de la LOPD*)
- Estructura del fichero principal (*tipos de datos personales contenidos en el fichero*)
- Información sobre el fichero o tratamiento
  - ☐ Finalidad y usos previstos.
  - ☐ Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales, y procedencia de los datos.
  - ☐ Procedimiento de recogida.
  - ☐ Cesiones previstas.
  - ☐ Transferencias Internacionales.
  - ☐ Sistema de tratamiento.
  - ☐ Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
  - ☐ Descripción detallada de las copias de respaldo y de los procedimientos de recuperación.
  - ☐ Información sobre conexión con otros sistemas.
  - ☐ Funciones del personal con acceso a los datos personales.
  - ☐ Descripción de los procedimientos de control de acceso e identificación.
  - ☐ Relación actualizada de usuarios con acceso autorizado.

## *Anexo II: Nombramientos*

---

Se incluirán los nombramientos que afecten a los diferentes perfiles incluidos en este documento, como por ejemplo el del responsable de seguridad.

## *Anexo III: Autorizaciones de salida o recuperación de datos*

---

Adjuntar las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, incluyendo aquellas que se refieran a salidas que tengan un carácter periódico o planificado. Incluir asimismo, las autorizaciones relativas a la ejecución de los procedimientos de recuperación de datos.

## *Anexo IV: Delegación de autorizaciones*

---

En este anexo se ha de indicar las autorizaciones como la salida de dispositivos portátiles, la copia de seguridad o reproducción de documentos en soporte de papel, etc.

## *Anexo V: Inventario de soportes*

---

Se ha de indicar en este anexo la información relativa al inventario de soportes que no esté informado ya. Esos soportes deberán permitir identificar el tipo de información que contienen y permitirán que ésta sea inventariada y almacenada en un lugar cuyo acceso sea restringido al personal que se haya autorizado para ello en el documento de seguridad. El personal involucrado.

#### Anexo VI: Registro de incidencias

En este anexo se debe incluir la información del registro de incidencias, siempre y cuando este registro no esté informatizado, siguiendo lo indicado en la sección de *Procedimientos de notificación, gestión y respuesta ante las incidencias*.

#### Anexo VII: Encargados de tratamiento

En este anexo incluirá una copia del contrato que deberá firmar el encargado de tratamiento de los ficheros en el cual se especificará que los datos se tratarán siempre cumpliendo las especificaciones del responsable de los ficheros y nunca con fines distintos a los que se describan en este contrato.

#### Anexo VIII: Registro de entrada y salida de soportes

Se deberá incluir la información sobre el registro de entrada y salida de soportes al que se hace referencia en el apartado de *Gestión de soportes y documentos* de la sección de *Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento*, que es obligatorio a partir del nivel medio. En caso de que este registro esté informatizado se debe incluir la aplicación o ruta de acceso al archivo que contiene dicho registro.

#### Anexo IX: Medidas alternativas

En este anexo se deben de especificar qué medidas no se pueden adoptar de las exigidas por el RLOPD, las causas por las que no se pueden realizar y por último las medidas alternativas que se han llevado a cabo.

### 3.4. Consecuencias de no disponer del Documento de Seguridad

La consecuencia básica de no disponer de documento de seguridad, cuando estamos obligados a ello, es la imposición de una sanción por parte de la Agencia Española de Protección de Datos. En este caso, podría tratarse de una sanción grave por no cumplir con las medidas de seguridad del RLOPD y la sanción podría alcanzar los 300.000€.

### 3.5. ¿Debe actualizarse el documento de seguridad?

- Artículo 88.7 del RLOPD:

*“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, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.”*

Por 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 actual de la empresa.

### 3.6. ¿Es obligatorio que los empleados conozcan la existencia y contenido del documento de seguridad?

---

Toda persona con acceso a datos personales, o que intervenga en alguna fase del tratamiento de los mismos, debe ceñirse a lo establecido en el documento de seguridad, en el cual se establecerán claramente las funciones y obligaciones del personal. Artículo 9.1 R.D 994/1999.

Es responsabilidad del responsable del fichero adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento. Artículo 9.2 R.D 994/1999.

## 4. El personal involucrado

---

### 4.1. Responsable del fichero

---

El responsable del fichero es la persona o la empresa que se responsabiliza a garantizar el uso de los datos de carácter personal de manera acorde a la Ley Orgánica de Protección de Datos. Sobre él recaen la mayor parte de responsabilidades establecidas por la LOPD, que son , entre otras, las siguientes:

#### *Inscripción de ficheros*

---

Registrar los ficheros en el Registro General de Protección de Datos, para que se proceda a su inscripción.

#### *Calidad de los datos*

---

El responsable debe asegurarse de que los datos que se están tratando son adecuados y veraces, además de haber sido obtenidos de manera legal y utilizados para la finalidad para la que fueron recabados.

#### *Deber de guardar secreto*

---

Debe también garantizar que esos datos cumplen con los deberes de secreto y seguridad que se preestablecen.

#### *Deber de información*

---

Por otro lado debe informar a los usuarios a los que pertenecen los datos personales de que su información está siendo recogida y posteriormente obtener la autorización y consentimiento para el uso de los mismos.

#### *Atención de los derechos de los ciudadanos*

---

Por último, el responsable también debe facilitar el cumplimiento de los derechos de oposición al tratamiento, acceso, rectificación y cancelación de los que disponen los ciudadanos.

Cabe destacar por último, que puede que haya más de un responsable asignado a un mismo fichero.



## 4.2. Personal encargado del tratamiento

---

El personal encargado del tratamiento del fichero es la persona, empresa o entidad que manipula los ficheros que contienen datos de carácter personal y garantizan que se respete durante esta manipulación la LOPD y todos los derechos que les corresponde a los ciudadanos al respecto.

Dentro de este grupo se incluyen tanto al personal de seguridad como a cualquier otro que tenga acceso a los datos o pueda dar acceso al mismo a terceros.

## 4.3. Ciudadano o personal interesado o afectado

---

Esta es la persona física que se presenta como titular o propietaria de los datos personales que se almacenan en el fichero. Éste puede ejercer sus derechos de oposición al tratamiento, acceso, rectificación y cancelación. O sea, en resumen, posee la capacidad de controlar sus datos personales y de disponer y decidir sobre éstos.

## 5. Control de accesos

---

### 5.1. ¿Qué es el control de acceso?

---

Un sistema de control de acceso hace referencia a un sistema electrónico que restringe o permite el acceso de un usuario que se haya identificado previamente a un área o recurso específico. Es decir, el control de acceso consiste en la comprobación de que una entidad posee los derechos necesarios para poder acceder a un recurso que está solicitando.

Estos recursos pueden ser; **recursos físicos**, por ejemplo, el acceso a una habitación donde se ubican los servidores; **recursos lógicos**, por ejemplo, un sistema operativo o una aplicación informática específica.

### 5.2. Componentes

---

El control de acceso generalmente incluye tres componentes:

- **Mecanismo de autenticación:** Este primer mecanismo consiste en identificar primero quién es el usuario y que está accediendo al recurso y posteriormente validar y verificar la identidad del usuario mediante contraseñas, claves, escáneres biométricos o reconocimientos de voz.
- **Mecanismo de autorización:** Una vez autenticada la entidad, tiene que ser autorizada para poder acceder al recurso, es decir, puede que no posea los permisos o privilegios para poder acceder a ese recurso determinado.
- **Mecanismo de trazabilidad:** A veces el mecanismo de autorización no resulta suficiente para garantizar que el usuario tiene derecho a acceder al recurso. Mediante la trazabilidad se compensa esa carencia utilizando la espada de Damocles. Este mecanismo también sirve para identificar al responsable de una acción una vez ya se ha realizado.

### 5.3. Control de acceso para ficheros automatizados

---

#### *Artículo 89 - Funciones y obligaciones del personal – nivel básico*

---

- Las funciones y obligaciones de cada uno de los usuarios con acceso a los datos estarán definidas en el documento de seguridad.
- El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones

#### *Artículo 91 - Control de acceso – nivel básico*

---

- Los usuarios tendrán acceso sólo a aquellos recursos que precisen para el desarrollo de sus funciones.
- El responsable del fichero se encargará de que haya una relación actualizada entre los usuarios y los accesos para cada uno de ellos.
- El responsable del fichero se encargará de que un usuario no pueda acceder a recursos con derechos distintos a los autorizados.
- Solo el personal autorizado podrá alterar el acceso autorizado sobre los recursos.
- Si existe personal ajeno al responsable del fichero con acceso a los recursos estará sometido a las mismas condiciones y obligaciones que el personal propio.

#### *Artículo 99 - Control de acceso físico – nivel medio*

---

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

#### *Artículo 103 - Registro de accesos – nivel alto*

---

- En cada intento de acceso se guardará identificación, fecha, hora, fichero accedido, tipo de acceso y si ha sido autorizado o denegado.
- En caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
- Los mecanismos del registro están bajo control del responsable de seguridad.
- El periodo mínimo de conservación de datos registrados es 2 años
- El responsable de seguridad tendrá que revisar al menos 1 vez al mes la información de control y elaborar un informe de las revisiones y problemas detectados
- No será necesario el registro de acceso en caso de que el responsable del fichero sea una persona física y que el responsable del fichero garantice que únicamente él tiene acceso y trata los datos personales.

Nivel	Obligaciones
BÁSICO	Los usuarios sólo tienen acceso a los recursos que necesiten y estos no pueden acceder a recursos que no les corresponden.
MEDIO	<i>Las mismas indicaciones que para el nivel básico</i> , pero además, existe un control de acceso físico. Solo el personal autorizado podrá acceder a la sala donde se ubiquen los servidores donde estén alojadas las bases de datos.
ALTO	<i>Las mismas indicaciones que para el nivel básico y medio</i> , pero además, deben registrarse todos los accesos y estos deberán estar bajo el control del responsable de seguridad. Este además deberá redactar un informe mensual con los problemas que se han detectado. Los registros deberán conservarse mínimo dos años.

#### 5.4. Control de acceso para ficheros manuales

##### *Artículo 113 - Acceso a la documentación*

- Se limitará exclusivamente al personal autorizado.
- Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos con múltiples usuarios.

Nivel	Obligaciones
BÁSICO	<i>Se deberán cumplir las mismas indicaciones que para los ficheros automatizados de nivel básico.</i>
MEDIO	<i>Se deberán cumplir las mismas indicaciones que para los ficheros automatizados de nivel medio.</i>
ALTO	<i>Se deberán cumplir las mismas indicaciones que para los ficheros automatizados de nivel alto</i> , pero además, el acceso debe limitarse al personal autorizado. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos con múltiples usuarios.

### 6. Gestión de soportes y documentos

#### 6.1. Gestión de soportes para ficheros automatizados

##### *Artículo 92 - Gestión de soportes y documentos – nivel básico*

- Los soportes y documentos deberán permitir identificar el tipo de información que contienen, ser inventariados y solo ser accesibles por el personal autorizado.
- La salida de soportes y documentos fuera de los locales bajo el control del responsable del fichero deberá ser autorizada por el responsable del fichero.

- 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
- Siempre que vaya a desecharse algún documento o soporte con datos de carácter personal deberá procederse a destrucción o borrado.
- La identificación de soportes con datos de carácter personal especialmente sensibles podrá ser realizada utilizando sistemas de etiquetado comprensibles para los usuarios con acceso autorizado pero que dificulten la identificación del resto de personas.

#### *Artículo 97 - Gestión de soportes y documentos – nivel medio*

- Deberá establecerse un sistema de registro de entrada de soportes que permita conocer el tipo de documento o soporte, el emisor, la fecha y hora, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción.
- Se dispondrá también de un sistema de registro de salida de soportes que permita conocer los mismos datos expuestos en el punto anterior.

#### *Artículo 101 - Gestión y distribución de soportes – nivel alto*

- La identificación de soportes se realizará utilizando sistemas de etiquetado comprensibles para los usuarios con acceso autorizado y difíciles de interpretar para el resto de personas.
- La distribución de los soportes se realizará cifrando dichos datos o usando mecanismos que garanticen que la información no sea accesible o manipulada en el transporte.
- Deberá evitarse el tratamiento de datos en dispositivos portátiles que no permitan su cifrado, en caso de que sea necesario se hará constar en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos.

Nivel	Obligaciones
BÁSICO	Se debe identificar siempre el tipo de datos que se contienen y además existirá un inventario de soportes. Este inventario se almacenará en un lugar restringido y toda salida de soportes deberá estar autorizada.
MEDIO	<i>Las mismas indicaciones que para el nivel básico, pero además, se deberá registrar la entrada y salida de soportes.</i>
ALTO	<i>Las mismas indicaciones que para el nivel básico y medio, pero además, los soportes solo se distribuirán de manera cifrada o mediante mecanismos que garanticen que la información no sea legible ni manipulada por terceros.</i>

## 6.2. Gestión de soportes para ficheros no automatizados

---

### *Artículo 106 - Criterios de archivo*

---

- El archivo de soportes se realizará usando criterios que garanticen 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 los casos sin norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación del archivo.

### *Artículo 107 - Dispositivos de almacenamiento*

---

- Los dispositivos de almacenamiento de los documentos deberán disponer de mecanismos que obstaculicen su apertura.
- Cuando las características físicas no permitan adoptar esta medida será el responsable del fichero quien adoptará medidas que impidan el acceso a personas no autorizadas.

### *Artículo 108 - Custodia de los soportes*

---

- La persona que se encuentre a cargo de la documentación deberá custodiarla e impedir en todo momento que pueda ser accedida por una persona no autorizada

### *Artículo 111 - Almacenamiento de la información*

---

- Los elementos en los que se almacenen los ficheros, como archivadores o armarios, deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso con un sistema de apertura mediante llave u otro dispositivo.
- Si no fuera posible cumplir lo establecido en el punto anterior, el responsable adoptará medidas alternativas que 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.

Nivel	Obligaciones
BÁSICO	<i>Se deberán cumplir las mismas indicaciones que para los soportes automatizados de nivel básico, pero además se aplicarán criterios que permitan la conservación, localización y consulta de estos soportes. Se deberán poner mecanismos que obstaculicen la apertura de los dispositivos de almacenamiento</i>
MEDIO	
ALTO	<i>Se deberán cumplir las mismas indicaciones que para los soportes automatizados de nivel alto, pero además, el acceso debe limitarse al personal autorizado. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos con múltiples usuarios.</i>

## 7. Copias de Seguridad

### 7.1. ¿Qué es una Copia de Seguridad?

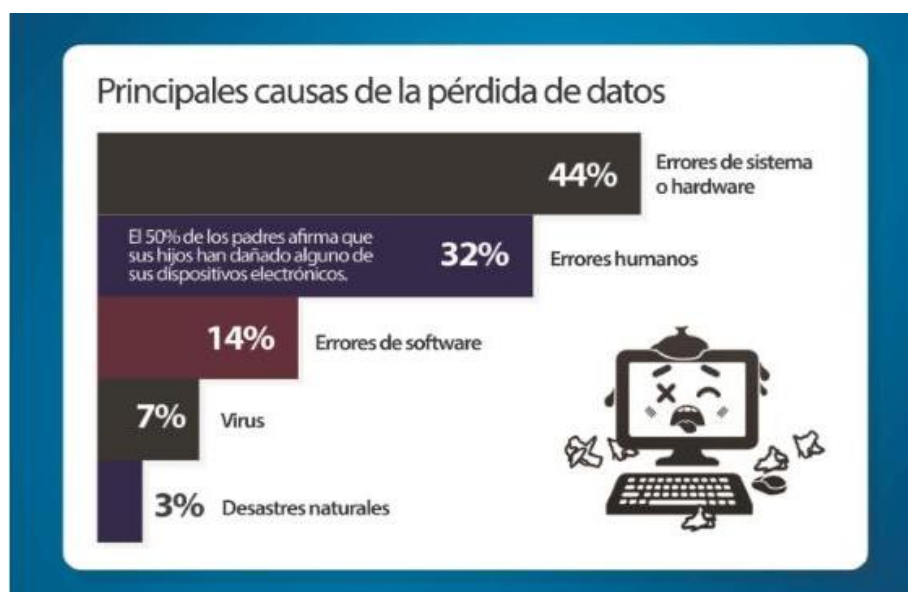
Una copia de seguridad es un **duplicado de los datos originales** que genera nuestro sistema. Todo esto con la finalidad de disponer de estos datos cuando sea necesario, siendo estos útiles e imprescindibles en diversas situaciones.

### 7.2. ¿Por qué crear Copias de Seguridad?

En primer lugar, podemos necesitar de estas copias cuando se producen **pérdidas de datos** debidas a catástrofes naturales o informáticas o simplemente a **ataques** de sistemas externos., ya que necesitaremos recuperar los datos que hemos perdido. O simplemente necesitemos restaurar o limpiar una cantidad pequeña de datos que pueden haberse eliminado de manera accidental o simplemente corrompido.

Pero las copias de seguridad no son sólo útiles para recuperar información pérdida o dañada, sino que también permiten guardar una información histórica, de una manera más económica que utilizando discos duros, que permita un **traslado de la información** a una ubicación distinta a la actual.

Aun así, la **pérdida de datos** sigue siendo la razón con más peso por la que se deben realizar copias de seguridad, ya que el 66% de los usuarios de Internet han sufrido alguna vez una.



Es necesario e imprescindible combatir esta pérdida de datos mediante copias de seguridad ya que si no lo hacemos, esto puede generarnos problemas serios para nuestra empresa: **problemas legales**, como denuncias de clientes debido a una mala gestión de sus datos o el incumplimiento de la ley de preservación de datos; **problemas administrativos**, como pérdida de datos de clientes o pérdida de información interna de la empresa o **problemas económicos**, como la caída de la página web, la pérdida de clientes o la paralización de departamentos que trabajan con las BD.

### 7.3. Almacenar Copias de Seguridad

---

Todas estas copias de seguridad es posible almacenarlas en diversos sistemas de almacenamiento:

- Disco duro interno en exclusividad (no solo una carpeta en nuestro sistema)
- Disco duro externo
- Disco duro virtual o Cloud.
- Discos de Dvds/Cds7

Dependiendo del tipo de dato que estemos almacenando podemos hacer la copia de seguridad en un sitio o en otro (archivos, servidores, bases de datos...)

### 7.4. La Ley Orgánica de Protección de Datos y las Copias de Seguridad

---

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

Nivel	Tipo de dato	Alcance
BÁSICO	Datos de carácter personal (nombres, emails, direcciones, etc.)	Cualquier organización, empresa o institución
MEDIO	Datos referidos a la comisión de infracciones administrativas o penales, Hacienda Pública, Servicios Financieros, solvencia patrimonial y crédito	Administración pública, entidades financieras y sector jurídico, entre otros
ALTO	Datos relacionados con la ideología, origen racial, salud, creencias, filiación sindical, religión y sexo	Centros de formación, partidos políticos, salud, RR.HH., clubs y agrupaciones de ocio y todas las empresas que gestionan sus nóminas

Para cada nivel se imponen una serie de obligaciones en materia de Backup desde la propia realización del Backup, pasando por garantizar la restauración de los datos al momento anterior de producirse la pérdida, hasta la obligación de disponer de un Backup externalizado.

Obligaciones	Niveles		
	Básico	Medio	Alto
Backup al menos una vez por semana	X	X	X
Garantizar restauración de los datos al momento antes de producirse la pérdida	X	X	X
Requiere autorización para iniciar el proceso de recuperación de datos		X	X
Almacenamiento externo de los datos y procedimientos de restauración			X

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. *Valor: 900-40.000€*
- **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. *Valor: 40.000-300.000€*
- **MUY GRAVES:** Comunicación o cesión no permitida de datos personales, vulneración de principios para datos especialmente protegidos. *Valor: 300.000-600.000€*



## 7.5. Estrategias de backup

---

Estrategia	Ventajas	Inconvenientes
Completa	Se copian todos los ficheros	Consumo de espacio
	Fácil recuperación total y parcial del sistema	
Incremental	Más rápida que las copias completas	Se pueden copiar ficheros cuyo contenido no ha cambiado
	Consume menos espacio	
	Permite control de versiones en un mismo fichero	Para recuperar un sistema, se necesitan todas las copias incrementales además de la completa
Diferencial	Todas las de la incremental, consumiendo menos espacio	La restauración de ficheros individuales consume tiempo ya que se deben buscar en las copias incrementales
		Todas las de las incrementales menos la primera
		No todas las herramientas permiten estas copias

## 7.6. Plan de prevención genérico

---

### 7.6.1. Cómo aplicarlo

---

1. Copia de nivel 0: primer lunes de cada mes.
2. Copia de nivel 1: resto de lunes y primer martes del mes.
3. Copia nivel 2: resto de días basándonos en la copia de nivel 1 más reciente.

### 7.6.2. Cómo recuperar los archivos

---

1. Recuperar todos los ficheros almacenados en la copia de nivel 0 más reciente.
2. Recuperar ficheros de la copia de nivel 1 de la semana actual.
3. Recuperar archivos de la última copia de nivel 2 realizada.

## 7.7. Conclusiones

---

Las copias de seguridad son necesarias y realmente útiles, además de obligatorias en algunos de los casos. Por lo que es necesario estudiar el tipo de nivel que conforman nuestros datos.

Establecer una estrategia de almacenamiento, búsqueda y recuperación de cualquier información de nuestra empresa, supone un coste, pero si se realiza correctamente, el coste será amortizado rápidamente, la recuperación o la búsqueda de la información será eficiente al mismo tiempo que la política de copias de seguridad se unificarán y simplificarán.

Evitaremos pérdidas de tiempo inútiles en localizar documentos, en restaurarlos en caso de accidente y conseguiremos un control eficiente de toda nuestra base de datos.

## **8. Seguimiento y control (Auditoría LOPD)**

---

### **8.1. ¿Qué es una Auditoría de Protección de Datos?**

---

La Auditoría de Protección de Datos es una inspección o revisión de las medidas (informáticas, físicas o de archivos, así como organizativas y documentales) y el tratamiento que realiza una empresa de los datos que esta maneja. Esta inspección lo que busca es determinar si se han establecido, si son adecuadas y si se cumplen las medidas de seguridad recogidas según la Ley Orgánica de Protección de Datos de Carácter Personal.

Su realización es obligatoria para ficheros de nivel medio y alto y debe realizarse al menos cada dos años. Excepcionalmente, si se han realizado modificaciones sustanciales en el sistema de información, deberá realizarse una auditoría para comprobar la adecuación, adaptación y eficacia de las medidas de seguridad. Esta auditoría iniciará el cómputo de dos años.

Se debe someter a una auditoría cada dos años. Es obligatorio Una multa económica, que oscila entre los **30.001 euros y los 40.000 euros**, y que puede imponer el órgano competente, que en este caso, es la **Agencia Española de Protección de Datos**

### **8.2. ¿Quién debe realizar la auditoría?**

---

El Real Decreto 1720/2007 no especifica ni el perfil de profesional para realizar la auditoría ni si el mismo debe tener alguna calificación especial. Simplemente indica que la auditoría será **interna o externa**. En cualquier caso sería recomendable que la realizara algún profesional o grupo de profesionales, internos o externos, con conocimientos de la LOPD y el Real Decreto 1720/2007, y con un perfil **jurídico-técnico** suficiente para analizar las medidas de seguridad implementadas así como su adecuación o no a la normativa vigente. Resulta también recomendable que el citado profesional acredite un nivel de conocimiento previo a través de algún sistema de certificación en protección de datos por alguna entidad externa e independiente.

### **8.3. ¿Cuáles son los pasos a seguir a la hora de realizar una auditoría?**

---

A pesar de que, como ya hemos comentado, es recomendable que la auditoría la realice alguien con conocimientos jurídicos, es importante también siempre conocer los pasos a seguir para poder prepararse para la auditoría de una manera correcta.

Se deberá en primer lugar, identificar los ficheros con datos personales, analizando los recursos (programas, equipos y soportes) donde se tratan dichos datos. También se deberá incluir los archivadores o lugares donde se alojen datos en papel.

Seguidamente, se debe concretar el nivel de seguridad aplicable a cada recurso, es decir, si el nivel es medio o alto.

A continuación, se deberá analizar las medidas de seguridad que se han aplicado y detectar posibles deficiencias en ellas.

Finalmente, se realizará un **informe de auditoría**.

A pesar que el deber de auditoría afecta únicamente a las medidas de seguridad, resulta recomendable que en este proceso se revise el cumplimiento de otras obligaciones en materia de protección de datos: cláusulas informativas y de consentimiento, contratos con proveedores o la formación al personal.

#### 8.4. Informe de Auditoría

---

El Informe de Auditoría deberá ser un documento que resuma de la Auditoría de Protección de Datos que se ha realizado. Deberá estar siempre a disposición de la Agencia Española de Protección de Datos. Este informe contendrá la siguiente información:

- Nivel de **adecuación** de las medidas y controles establecidos.
- **Deficiencias** detectadas y propuesta de medidas correctoras o complementarias.
- Datos, hechos y observaciones **en que se basen los dictámenes** alcanzados y recomendaciones propuestas.



El cliente siempre agradecerá que se le aporte un **Plan de Acción**, e incluso lo habrá exigido expresamente. Para ello lo que se puede hacer es calificar las recomendaciones en columnas o ámbitos diferentes: riesgo, plazo de solución, coste y dificultades

## 9. Bibliografía

---

[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)

[http://noticias.juridicas.com/base\\_datos/Admin/rd1720-2007.t8.html](http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.t8.html)

<https://www.agpd.es/>

[https://es.wikipedia.org/wiki/Copia\\_de\\_seguridad](https://es.wikipedia.org/wiki/Copia_de_seguridad)

<http://blogthinkbig.com/crear-copias-de-seguridad/>

<https://www.osi.es/es/copias-de-seguridad-cifrado>

[http://www.adminso.es/index.php/4.3.1. Tipos y estrategias de copias](http://www.adminso.es/index.php/4.3.1._Tipos_y_estrategias_de_copias)

<http://www.rosello-mallol.com/auditoria-lopd-debo-hacerla/>

<https://legaltis.wordpress.com/2013/05/28/que-es-una-auditoria-de-proteccion-de-datos/>

[https://es.wikipedia.org/wiki/Control\\_de\\_acceso](https://es.wikipedia.org/wiki/Control_de_acceso)

<http://www.cuidatusdatos.com/obligacioneslopd/medidasseguridad/documentoseguridad/index.html>