Tema 7. Ley Orgánica de Protección de Datos

1. La Agencia de Protección de Datos

Qué es

La Agencia Española de Protección de Datos (AEPD) es 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.

Qué funciones tiene

La Agencia Española de Protección de Datos está encargada de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos (ARCO).

La Carta de Servicios es un documento que constituye el instrumento a través del cual 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, sobre los derechos que les asisten en relación con aquellos y sobre los compromisos de calidad en su prestación. La Carta de Servicios de la AEPD se encuentra disponible en su página web para descargar como PDF.

Funciones en relación con los afectados

- Atender a sus peticiones y reclamaciones.
- Informar de los derechos reconocidos en la Ley.
- Promover campañas de difusión a través de los medios.
- Velar por la publicidad de los ficheros de datos de carácter personal.

En relación con quienes tratan datos

- Emitir las autorizaciones previstas en la Ley.
- Requerir medidas de corrección.

- Ordenar, en caso de ilegalidad, 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 Autorizar las transferencias internacionales de datos.precise para el ejercicio de sus funciones.

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.

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 realizadas a través de correo electrónico o medios de comunicación electrónica equivalente (spam).
- Recibir las notificaciones de las eventuales quiebras de seguridad que se produzcan en los sistemas de los proveedores de servicios de comunicaciones electrónicas y que puedan afectar a datos personales.

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 en la materia.
- Control y observancia de lo 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.

Componentes

- **Directora**
    - La Directora ostenta la representación de la Agencia y sus actos se consideran como actos propios de la Agencia. Sus resoluciones ponen fin a la vía administrativa y son recurribles ante la Sala de lo Contencioso de la Audiencia Nacional.
    - Funciones
        - *Dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia*, como resolver las inscripciones que deban practicarse 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*.
        - Diversas *funciones de gestión*, como aprobar gastos, ordenar pagos o ejercer el control económico-financiero de la Agencia.

- La Directora de la Agencia Española de Protección de Datos es asistida en el ejercicio de sus funciones por una *Unidad de Apoyo* integrada por las siguientes unidades:
  - *Adjunto al Director*: colabora con el Director en las relaciones institucionales que desarrolla la Agencia y con las diferentes unidades que conforman la institución.
  - *Gabinete Jurídico*: órgano encargado del asesoramiento jurídico al Director, así como a las subdirecciones generales.
  - *Área internacional*: asesoramiento y apoyo a la Dirección de la Agencia en materia de relaciones internacionales, representando a la Institución en diversos foros internacionales. Coordinación de la actividad internacional de las unidades de la Agencia.
  - *Gabinete de Comunicación y Prensa*: impulsa las relaciones con los medios de comunicación y difunde la actividad de la Agencia con objeto de fomentar una cultura de protección de datos entre ciudadanos y entidades, promoviendo la imagen institucional de este organismo.

- **El Consejo Consultivo**

  - Es el órgano colegiado de asesoramiento del Director, siendo éste elegido de entre sus miembros. Lo componen un total de 10 miembros nombrados por un periodo de cuatro años. Lo preside el Director de la Agencia y actúa como secretaria la titular de la Secretaría General.
  - El Consejo Consultivo se reúne cuando lo convoca el Director y, al menos, una vez cada seis meses. Emite informe en todas las cuestiones que le someta el Director, pudiendo formular propuestas en materia de protección de datos.

- **Registro General de Protección de Datos**

  Tiene las funciones 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, así como la autorización de conservación de datos para fines históricos, estadísticos o científicos.

- **Secretaría General**
    - Funciones
        - Dar soporte y apoyo al adecuado funcionamiento de las distintas unidades de la Agencia.
        - Elaboración de informes y propuestas.
        - Ejercer la secretaría del Consejo Consultivo.
    - Se organiza en diferentes áreas:
        - *Área de Informática*: se encarga entre otras cosas del soporte a los servicios de atención al ciudadano, como la página web de la Agencia, así como del registro de los ficheros de carácter personal (una aplicación permite al ciudadano enviar un formulario de alta de ficheros).
        - *Área de Atención al Ciudadano*: tiene funciones como la de orientación y atención al ciudadano, reparto de encuestas, etc.
        - *Área de Administración General*: se encarga de la gestión económico-administrativa de la Agencia.
        - *Documentación y estudios*: se ocupa de la notificación de resoluciones de expedientes que firma la Directora, de actualizar el fondo de documentación sobre legislación, etc.

- **Inspección de Datos**
    - Funciones que lleva a cabo:
        - *Tramitar los procedimientos relativos al ejercicio de la potestad sancionadora* que a la Agencia le atribuyen la LOPD (sobre protección de datos), la LSSI (sobre spam y cookies) y la LGT (sobre llamadas automáticas sin intervención humana o mensajes de fax, con fines de comunicación comercial).

        - *Tutelar los derechos de acceso, rectificación, cancelación y oposición de los ciudadanos* (ARCO).

    - Se organiza en:
        - *Inspección:* los funcionarios que ejercen la función de inspección realizan visitas de inspección, en los locales o sede del inspeccionado, o donde se encuentren ubicados los ficheros, en su caso.
        - *Instrucción*: los funcionarios que ejercen la función instructora se ocupan de la tramitación de los procedimientos sancionadores y de declaración de infracción por las Administraciones Públicas.
        - *Tutela de derechos ARCO*: en esta área se tramitan las reclamaciones que presentan los ciudadanos en relación con el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición.

Ejemplo: protección de datos en la UA

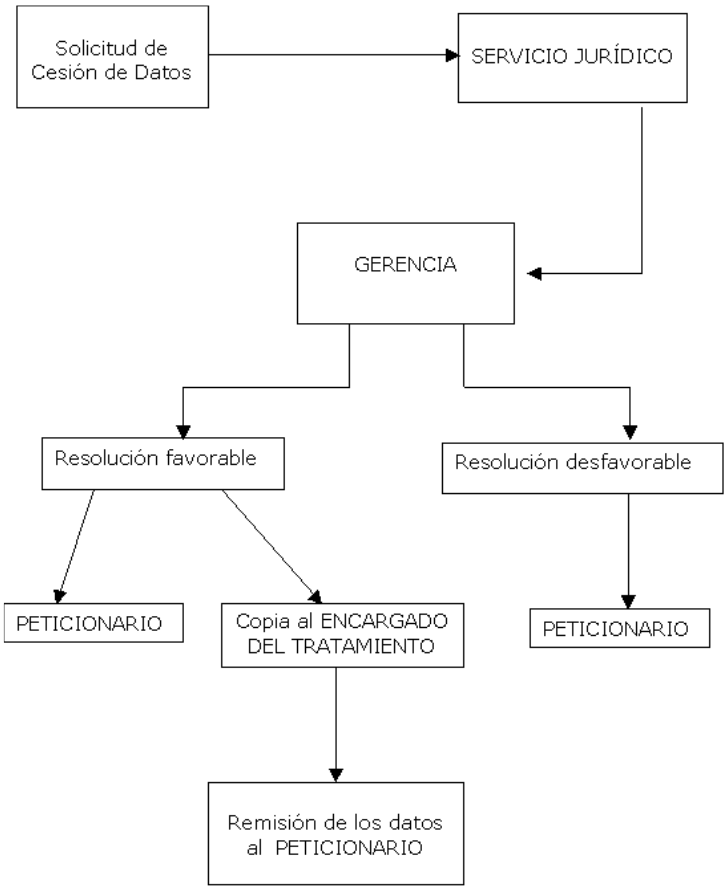
Veamos ahora como ejemplo cómo la Universidad de Alicante protege los datos de carácter personal.

En la Universidad de Alicante, la última resolución sobre la creación y modificación de ficheros de carácter personal es la redactada por el rector de la Universidad de Alicante el 26 de septiembre de 2014.

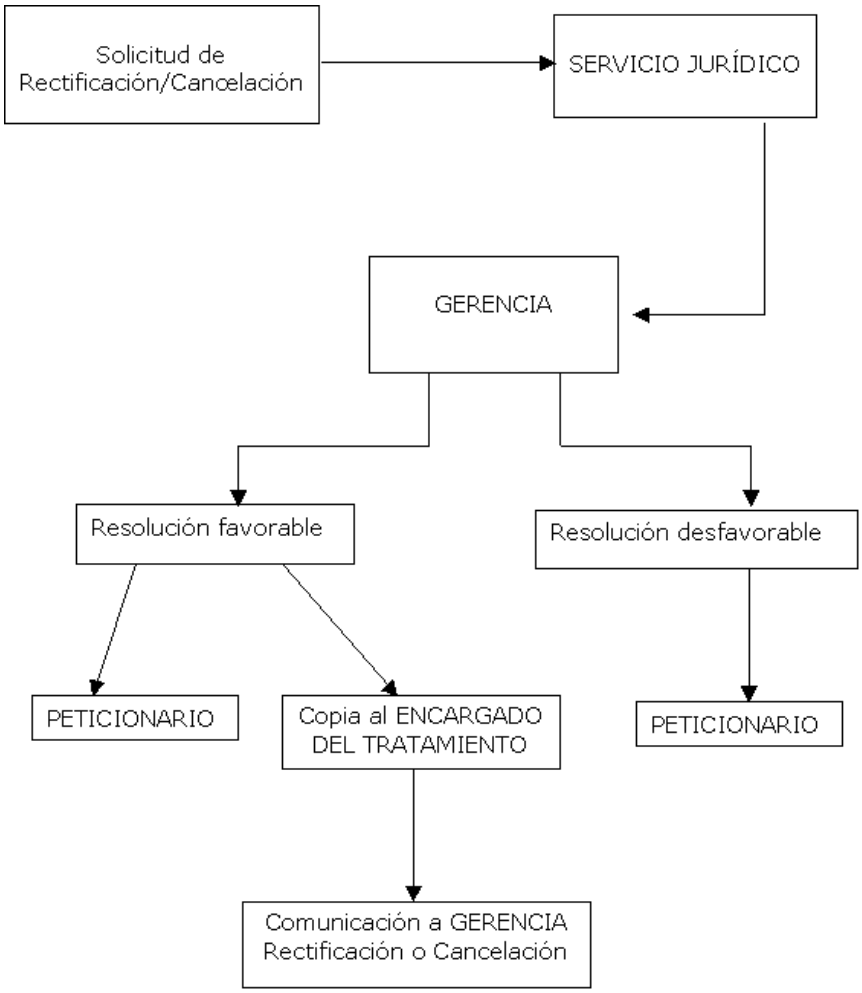
Procedimiento interno de protección de datos de carácter personal

Las cesiones de ficheros de carácter personal han de ser autorizadas por la Gerencia de la Universidad, tal como vemos a continuación:

- Organigrama de solicitud de cesión de datos de carácter personal



- Organigrama de rectificación/cancelación de datos



Legislación

La protección de ficheros de carácter personal está regulada por:

- LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley de Propiedad Intelectual.
- LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- REAL DECRETO 1720/2007 Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Registro de ficheros

Por qué registrar ficheros

Imaginemos que tenemos que guardar los datos de los clientes de nuestra empresa en una base de datos. Se trataría pues de un fichero de carácter personal. El art. 26 de la Ley Orgánica de Protección de Datos establece como requisito obligatorio, carácter previo a la creación de fichero de datos, la comunicación al Registro de la Agencia Española de Protección de Datos de la creación de ficheros de carácter personal que vayamos recolectando. Ello significa, que antes de crear nuestra base de datos con la información sobre nuestros clientes, tenemos que inscribir dicho fichero en el registro de la Agencia.

No solicitar la inscripción de los ficheros de datos de carácter personal en el RGPD constituye infracción leve, con arreglo a lo dispuesto en el artículo 44.2.b) de la LOPD.

Según el artículo 58 del RLOPD, la inscripción de los ficheros deberá encontrarse actualizada en todo momento, por lo que cualquier modificación que afecte al contenido de la inscripción, así como su supresión deberá ser notificada a la AEPD para proceder a la inscripción de la modificación o a la cancelación del fichero.

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.

Cómo se hace el registro de ficheros

Para realizar la inscripción inicial del fichero y, en su caso, la posterior modificación o supresión de la inscripción, se encuentra disponible en la Sede Electrónica de la Agencia Española de Protección de Datos el Servicio Electrónico *NOTA* a través del que deberán

efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos.

Este formulario permite la presentación 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 se puede presentar la notificación a través de Internet, para lo cual se deberá remitir a la Agencia la Hoja de solicitud correspondiente al envío realizado debidamente firmada.

Asimismo, permite notificar de forma simplificada, los ficheros de titularidad privada de comunidades de propietarios, clientes, pacientes, etc. A través de esta opción, el formulario electrónico muestra una notificación precumplimentada que podrá completar, o en su caso, adaptar a la situación concreta del fichero a notificar.

3. El documento de seguridad

El RLOPD especifica que se puede disponer de un solo documento que incluya todos los ficheros y tratamientos con datos personales de los que una persona física o jurídica sea responsable, un documento por cada fichero o tratamiento, o los que determine el responsable atendiendo a los criterios organizativos que haya establecido. Cualquiera de las opciones puede ser válida.

El contenido de este documento queda estructurado como sigue:

- Ámbito de aplicación del documento.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
- Información y obligaciones del personal.
- Procedimientos de notificación, gestión y respuestas ante las incidencias.
- Procedimientos de revisión.

Este documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de <nombre del responsable>, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en

todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

4. El personal involucrado

CONTROL DE ACCESO

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. Exclusivamente esta persona está autorizada (o denominación de su puesto de trabajo) para conceder, alterar o anular el acceso autorizado.

Se han de especificar los procedimientos para solicitar el alta, modificación y baja de las autorizaciones de acceso a los datos, indicando qué persona (o puesto de trabajo) concreta tiene que realizar cada paso. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista deberá mantenerse actualizada.

De existir personal ajeno al responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

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. El mecanismo que permita este registro estará bajo control directo del responsable de seguridad, sin que se deba permitir, en ningún caso, la desactivación del mismo.Los datos del registro de accesos se conservarán durante determinado periodo, que deberá ser al menos de dos años.

No es preciso que estos datos se almacenen. El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe.

No será necesario el registro de accesos cuando:

- El responsable del fichero es una persona física
- El responsable del fichero garantice que sólo él tiene acceso y trata los datos personales.
- Se haga constar en el documento de seguridad.

5. Control de accesos

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 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.”

Con fecha 3 de noviembre de 2015 se solicitó información al responsable del establecimiento, que manifestó lo siguiente:

“Las cámaras exteriores están situadas y orientadas hacia la parcela, únicamente toman imágenes de la zona inmediata al exterior del edificio y sus accesos, todos ellos dentro de la propia parcela.“

6. Gestión de soportes y documentos

Entre las medidas de seguridad de nivel básico, el Reglamento expone en su artículo 92, respecto de la gestión de soportes y documentos, que:

“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.”

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.”

7. Copias de seguridad

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

Las copias de seguridad se necesitarán en dos posibles casos:

- Cuando se producen **pérdidas de datos** debidas a catástrofes naturales o informáticas o simplemente a ataques de sistemas externos.
- Cuando necesitemos restaurar o limpiar datos que pueden haberse eliminado de manera accidental o simplemente corrompido.

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**: denuncias de clientes debido a una mala gestión de sus datos o el incumplimiento de la ley de preservación de datos.
- **Problemas administrativos**: pérdida de datos de clientes o pérdida de información interna de la empresa.
- **Problemas económicos**: por ejemplo, la caída de la página web, la pérdida de clientes o la paralización de departamentos que trabajan con las BD.

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…)

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€*

Para prevenir estas sanciones económicas se plantean las siguientes **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	Para recuperar un sistema, se necesitan todas las copias incrementales además de la completa
	Permite control de versiones en un mismo fichero	La restauración de ficheros individuales consume tiempo ya que se deben buscar en las copias incrementales
Diferencial	Todas las de la incremental, consumiendo menos espacio	Todas las de las incrementales menos la primera
		No todas las herramientas permiten estas copias

Plan de prevención genérico, ¿cómo aplicarlo?

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

Y cómo recuperar los archivos:

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

En conclusión, 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 LODP)

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, sino, la multa económica oscila entre los 30.001 euros y los 40.000 euros, impuesto por la **Agencia Española de Protección de Datos.**
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.

Pasos para realizar una auditoría:

- 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.

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: riego, plazo de solución, coste y dificultad.

9. Bibliografía

- Web de la Agencia Española de Protección de datos: www.agpd.es

- Web del servicio de Informática de la UA sobre la protección de ficheros de carácter personal: https://si.ua.es/es/normativa/proteccion-de-ficheros-de-datos-de-caracter-personal.html

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html

- Resolución de fecha-20-10-2016 Artículo-9-LOPD: http://www.agpd.es/portalwebAGPD/resoluciones/admon_publicas/ap_2016/common/pdfs/AAPP-00024-2016_Resolucion-de-fecha-20-10-2016_Art-ii-culo-9-LOPD.pdf)

- Resolución de fecha-22-12-2016 Artículo-12-LOPD: http://www.agpd.es/portalwebAGPD/resoluciones/admon_publicas/ap_2016/common/pdfs/AAPP-00034-2016_Resolucion-de-fecha-22-12-2016_Art-ii-culo-12-LOPD.pdf

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

- Página de Wikipedia sobre la copia de seguridad: https://es.wikipedia.org/wiki/Copia_de_seguridad

- Entrada de blog sobre las copias de seguridad: http://blogthinkbig.com/crear-copias-de-seguridad/

- Página web sobre las copias de seguridad: https://www.osi.es/es/copias-de-seguridad-cifrado

- Página web sobre los tipos de copias: http://www.adminso.es/index.php/4.3.1._Tipos_y_estrategias_de_copias

- Guía de la seguridad de datos de la AGPD: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

- Página web sobre la auditoría: http://www.rosello-mallol.com/auditoria-lopd-debo-hacerla/

- Página web sobre la auditoría: https://legaltis.wordpress.com/2013/05/28/que-es-una-auditoria-de-proteccion-de-datos/