

Protección de Datos Personales

Formación

Derecho.com

Objetivos de la sesión

- ¿Cuáles son las principales obligaciones que imponen la LOPD y el Reglamento de Seguridad?
- Resolución de dudas.

La protección de datos de carácter personal

Marco jurídico

- Artículo 18.1 de la Constitución española. Garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.
- Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD).

Marco jurídico

- 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 (**Reglamento de Seguridad**).
- Instrucciones y Memorias de la Agencia Española de Protección de Datos.
- Jurisprudencia de Juzgados y Tribunales.

Objeto de la Ley

- Garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las **personas físicas**, y especialmente de su honor e intimidad personal y familiar.

Conceptos básicos



Conceptos básicos

Dato de carácter personal:

- (LOPD): Cualquier información concerniente a personas físicas identificadas o identificables.
- (Reglamento de Seguridad): Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Conceptos básicos

Datos de carácter personal relacionados con la salud:

- Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

Ejemplos: informaciones relativas al abuso del alcohol o al consumo de drogas; afecciones; alergias; etc.

Conceptos básicos

Fichero:

- 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.

Ejemplos: Bases de datos; todo conjunto de datos personales almacenado en servidores u otros equipos informáticos y en archivadores de documentos.

Conceptos básicos

Tratamiento de datos:

- Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Cesión o comunicación de datos:

- Tratamiento de datos que supone su revelación a una persona distinta del interesado.

Conceptos básicos

Responsable del Fichero:

- 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 lo realice materialmente.

Afectado o interesado:

- Persona física titular de los datos que sean objeto del tratamiento.

Conceptos básicos

Responsable de Seguridad:

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

Encargado del tratamiento:

- La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trata 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.

Esquema de tratamiento



Esquema de tratamiento habitual

Responsable del Fichero

Encargado del Tratamiento

Deber de velar por el cumplimiento de las garantías.

Afectados o interesados

Cesionario



Principios básicos

Principios básicos

Calidad:

- Los datos personales deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades para las que se han recogido.

Actualidad y Exactitud:

- Los datos personales incorporados a un fichero han de responder a la situación actual del afectado.

Principios básicos

Finalidad:

- Los datos no pueden utilizarse para finalidades distintas a aquellas para las que han sido recabados.

Consentimiento:

- El tratamiento de los datos requiere el consentimiento inequívoco (tácito o expreso) del afectado.

Principios básicos

Información:

- Cuando se recojan datos de carácter personal debe informarse al interesado sobre:
 - Existencia de un fichero.
 - Finalidad de la recogida de datos.
 - Destinatario de los datos.
 - Procedimiento para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Principios básicos

Seguridad:

- El Responsable del Fichero adoptará 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.

Deber de secreto:

- El Responsable del Fichero y quienes intervengan en cualquier fase del tratamiento de los datos están obligados al secreto profesional respecto a los mismos y al deber de guardarlos.

Esta obligación subsiste incluso después de haber finalizado la relación con el titular del fichero.

¿Cómo adecuar una empresa o institución a la normativa de protección de datos?



Pasos a seguir

- Notificar los ficheros ante la Agencia Española de Protección de Datos.
- Adecuar los procedimientos internos a las exigencias legales.
- Elaborar el Documento de Seguridad.

Pasos a seguir

- Otras obligaciones relevantes:
 - Difusión de las funciones y obligaciones del personal.
 - Firmar contratos de tratamiento de datos.
 - Realizar controles periódicos (cada seis meses).
 - Realizar auditorías de protección de datos bianuales.

Obligación de notificación de ficheros

Obligación de notificación

- ¿En que consiste la obligación?
 - Notificación previa a la creación del fichero.
 - Objeto de la notificación.
 - Ficheros que contienen datos de carácter personal.
 - Se notifican los campos, no los datos concretos.
 - Se indica quien es el responsable del fichero; donde pueden ejercerse los derechos del afectado; los encargados del tratamiento; el nombre y las finalidades del fichero; cómo y de quien se obtienen los datos; el sistema de tratamiento utilizado; el nivel de medidas de seguridad aplicable y las posibles cesiones o transferencias internacionales de datos.

Adecuación de los procedimientos internos



Adecuación de los procedimientos internos

- **Obtención de los datos:** ¿De dónde podemos obtener datos personales?
 - a) El propio interesado o su representante (Formularios o impresos, entrevistas).
 - b) Fuentes accesibles al público.
 - c) Otra persona (física o jurídica) distinta del afectado.

Adecuación de los procedimientos internos

- **Obtención de los datos:** Deberá mediar el consentimiento informado (avisos legales).

Excepciones: El consentimiento no es necesario cuando:

- a) Expresamente lo prevea una ley:
 - Para satisfacer una necesidad legítima del responsable del fichero.
 - Cuando el tratamiento es necesario para el cumplimiento de un deber legal del responsable del fichero.
- b) Se obtengan de fuentes de acceso público y exista un interés legítimo.

Adecuación de los procedimientos internos

- c) Se recojan para celebrar un contrato o precontrato, o durante una relación negocial, laboral, o administrativa.
- d) Se recojan para el ejercicio de las funciones propias de las AA.PP. en el ámbito de sus competencias.

Adecuación de los procedimientos internos

Cuando se recaban de una tercera empresa:

- Supuesto de cesión de datos.
- Necesidad de contar con el consentimiento del interesado.
- Consentimiento nulo: cuando la información que se facilite no permita al interesado conocer la finalidad a que destinarán los datos o el tipo de actividad del cesionario.
- Conveniencia de firmar siempre con la empresa cedente un contrato de cesión de datos.

Excepciones: No se requiere el consentimiento en los siguientes casos:

- Cuando la cesión está autorizada en una ley.
- Cuando se trate de datos recogidos de fuentes accesibles al público.

Adecuación de los procedimientos internos

Quando se recaban de Registros Públicos y Fuentes Accesibles al Público:

- Ficheros cuya consulta puede ser realizada por cualquier persona.
- La información de una fuente de acceso público no puede completarse por otras vías.

Tienen la consideración de fuentes accesibles al públicos (*numerus clausus*):

- Censo promocional.
- Guías de servicios de comunicaciones electrónicas.
- Listas de personas pertenecientes a grupos profesionales: nombre, título, profesión, actividad, grado académico, dirección profesional (domicilio postal, teléfono, fax y e-mail) y pertenencia al grupo.
- Diarios y Boletines Oficiales.
- Medios de comunicación social.

Adecuación de los procedimientos internos

- Las fuentes de acceso público que se editan en forma de libro o algún otro soporte físico pierden el carácter de fuente accesible con la nueva edición que se publique.
- Cuando los datos incluidos en fuentes accesibles al público se obtengan telemáticamente, ésta perderá el carácter de fuente de acceso público en el plazo de 1 año, desde la obtención.
- Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero, dentro de los 3 meses siguientes al momento del registro de los datos, del contenido y finalidad del tratamiento, de la procedencia de los datos, así como de los derechos que le asisten.

Adecuación de los procedimientos internos

- No será necesario informar, cuando expresamente una ley lo prevea o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Adecuación de los procedimientos internos

Tratamiento de datos:

- Sujeción a las finalidades declaradas.
- Implementación de medidas de seguridad.
- Cancelación de los datos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrado.

Documento de Seguridad



Documento de Seguridad

- **Concepto:** Documento que recoge las medidas de índole técnica y organizativa, de obligado cumplimiento para el personal con acceso a los sistemas de información.
- **Niveles de Seguridad:**
 - Básico
 - Medio
 - Alto



Documento de Seguridad

Nivel básico: Cualquier dato de carácter personal.

Nivel medio:

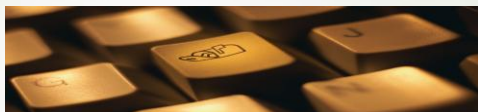
- Infracciones administrativas o penales.
- Ficheros de solvencia patrimonial y crédito (RAI, ASNEF, etc.).
- Los que las Administraciones tributarias tienen en relación con sus potestades tributarias.
- Datos de las entidades financieras para la prestación de servicios financieros.
- Datos propiedad de la Seguridad Social o las mutuas de accidentes de trabajo para el ejercicio de sus competencias.
- Evaluación de la personalidad o el comportamiento del individuo.

Documento de Seguridad

Nivel Alto:

- Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Se puede aplicar el nivel básico cuando:
- Sólo se tengan para transferir dinero a la entidad a la que el afectado pertenece.
 - Formen parte de ficheros no automatizados sin guardar relación con su finalidad.
 - Grado de discapacidad o invalidez del afectado para cumplir con deberes públicos.
- Datos para fines policiales que se recaban sin consentimiento del afectado.
 - Datos derivados de actos de violencia de género.
 - Datos de tráfico y localización de los servicios de comunicaciones electrónicas (Sólo medida de registro de accesos).

Medidas de seguridad aplicables a los ficheros y tratamientos automatizados



Medidas de Nivel Básico

1. Funciones y obligaciones del personal.

Las funciones y obligaciones de los usuarios con acceso a los datos de carácter personal deben recogerse en el Documento de Seguridad.

También aparecerán las personas que pueden conceder autorizaciones.

El personal debe conocer sus funciones y obligaciones, así como las consecuencias en caso de incumplirlas.

2. Registro de incidencias.

Debe existir un procedimiento de notificación y gestión de incidencias, así como un Registro donde se hará constar:

Tipo de incidencia, momento en que se ha producido o detectado, la persona que realiza la notificación, a quien se le comunica, los efectos derivados y las medidas correctoras.



Medidas de Nivel Básico

3. Control de acceso.

-Los usuarios sólo pueden acceder a aquellos datos que requieran para el ejercicio de sus funciones.

-Relación actualizada de usuarios con acceso autorizado a los sistemas de información.

-En el Documento de Seguridad se indicarán los usuarios que pueden alterar o anular los accesos autorizados del resto.

-El personal ajeno debe seguir las mismas condiciones de seguridad.



Medidas de Nivel Básico

4. Gestión de soportes y documentos.

-Los soportes deben identificar la información que contienen, ser inventariados y ser sólo accesibles al personal autorizado. Cuando no sea posible, se incluirá en el Documento de Seguridad.

-La salida de soportes y documentos debe ser autorizada por el responsable del fichero.

-Los soportes y documentos se desecharán de forma que no pueda recuperarse la información que contienen.



Medidas de Nivel Básico

5. Identificación y autenticación.

-Necesidad de implantar un mecanismo de identificación y autenticación personalizada. Si se utilizan contraseñas, estas se asignarán y distribuirán de forma confidencial, guardándose de forma ininteligible.

-Su periodo de vigencia no puede superar el año.



Medidas de Nivel Básico

6. Copias de respaldo y recuperación.

-Deben hacerse copias de seguridad, al menos, semanalmente.

-El procedimiento de recuperación de la información debe permitir volver al estado anterior a la incidencia. La grabación manual de los datos sólo será posible si se han visto afectados ficheros parcialmente automatizados.

-Cada 6 meses se debe revisar el procedimiento de realización de copias de seguridad y recuperación.



Medidas de Nivel Medio

1. Responsable de Seguridad.

Deberá designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas de seguridad contenidas en el Documento de Seguridad.

2. Auditoría.

Los ficheros con datos de nivel medio se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad que les son aplicables.



Medidas de Nivel Medio

3. Gestión de soportes y documentos.

Registro de entrada y salida de soportes, donde se hará constar: tipo y número de documento o soporte, fecha y hora, emisor, información que contiene, forma de envío, persona responsable de la recepción o envío.



4. Identificación y autenticación.

Se limitará el número de intentos de acceso fallido (se recomienda un máximo de cinco).



5. Control de acceso físico.

Sólo el personal autorizado puede acceder a los lugares donde se ubican los equipos que dan soporte a los sistemas de información.



Medidas de Nivel Medio

6. Registro de incidencias.

Debe anotarse el procedimiento realizado para recuperar los datos, la persona que lo ha ejecutado y los datos restaurados.



Medidas de Nivel Alto

1. Gestión y distribución de soportes.

-El etiquetado de los soportes debe ser sólo perfectamente comprensible para el personal autorizado.
-La distribución de soportes debe hacerse cifrando los datos o bien utilizando otros mecanismos análogos.
-Los datos contenidos en los equipos portátiles también se cifrarán.



2. Copias de respaldo y recuperación.

Debe conservarse una copia de seguridad de los datos en un lugar diferente de aquel donde se encuentran los equipos que los tratan.



3. Telecomunicaciones.

La transmisión de datos mediante redes de telecomunicaciones debe hacerse cifrando su contenido o bien utilizando otro medio que impida que dicha información pueda ser manipulada.



Medidas de Nivel Alto

4. Registro de accesos.

De cada acceso al fichero se guardará:

- Identificación del usuario
- Fecha y hora
- Fichero accedido
- Tipo de acceso y si éste ha sido autorizado o denegado.

-La información de estos registros de acceso se guardará un mínimo de dos años.



Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados



Medidas de Nivel Básico

1. Criterios de almacenamiento

La documentación debe archivarse según los criterios establecidos por su propia legislación. Cuando no exista norma aplicable, el responsable del fichero establecerá los criterios y procedimientos de actuación que deban seguirse para el archivo.



2. Dispositivos de almacenamiento

Los dispositivos de almacenamiento de los documentos deben disponer de mecanismos que obstaculicen su apertura. Si las características físicas de aquéllos no permiten adoptar esta medida, el responsable del fichero adoptará medidas que impidan el acceso de personas no autorizadas.



3. Custodia de soportes

Mientras la documentación no se encuentre archivada en los dispositivos de almacenamiento, 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 debe custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.



Medidas de Nivel Medio

1. Responsable de Seguridad

Deberá designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas de seguridad aplicables a estos ficheros.

2. Auditoría

Los ficheros con datos de nivel medio se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad que les son aplicables.



Medidas de Nivel Alto

1. Almacenamiento de la información

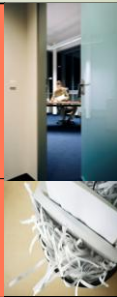
Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados, deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

Si las características de los locales de que dispone el responsable del fichero, no permiten cumplir con dicha obligación, éste adoptará medidas alternativas que, debidamente motivadas, se incluirán en el Documento de Seguridad.

2. Copia o reproducción

La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el Documento de Seguridad.

Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.



Medidas de Nivel Alto

3. Acceso a la documentación

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

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

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.

4. 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.



Derechos de los afectados



Derechos de los afectados

Los afectados tendrán los siguientes derechos:

- Derecho de acceso (1 mes / 10 días).
- Derecho de rectificación (10 días).
- Derecho de cancelación (10 días).
- Derecho de oposición.

* Necesidad de definir protocolos internos para dar respuesta a las peticiones de los interesados.



La Agencia Española de Protección de Datos (AEPD)



La Agencia Española de Protección de Datos

- 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.

La Agencia Española de Protección de Datos

- **Funciones:**
 - Velar por el cumplimiento de la legislación sobre protección de datos.
 - Emitir autorizaciones.
 - Dictar instrucciones.
 - Atender peticiones y reclamaciones.
 - **Potestad sancionadora** (infracciones leves, graves y muy graves: de 600 a 600.000 €).
 - Informar a las personas sobre sus derechos.
 - Requerir a los responsables de los ficheros la adecuación a la Ley de Protección de Datos.

La Agencia Española de Protección de Datos

- **Infracciones y sanciones:**
 - Recabar y tratar datos de carácter personal relativos a salud, origen racial o vida sexual cuando el afectado no haya consentido expresamente o no lo disponga una ley (300.506,05€ a 601.012,10€).
 - Comunicar o ceder datos de carácter personal cuando no esté permitido (300.506,05€ a 601.012,10€).

La Agencia Española de Protección de Datos

- Incumplimiento del deber de secreto respecto de datos de salud (300.506,05€ a 601.012,10€).
- Incumplimiento general del deber de secreto (601,01€ a 60.101,21€).
- Mantener los ficheros, locales, programas o equipos que contengan datos personales sin las debidas condiciones de seguridad (60.101,21€ a 300.506,05€).

Muchas gracias

DERECHO.COM