

# Datos al día

Boletín de actualidad jurídica en protección de datos

## ESPECIAL: REGLAMENTO DE LA LOPD

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.

### DEFINICIONES DEL REGLAMENTO

**Dato de carácter personal:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables

**Persona identificable:** toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.

**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, los referidos a su porcentaje de discapacidad y a su información genética.

**Destinatario o cesionario:** la persona física o jurídica, pública o privada u ór-

gano administrativo, al que se revelen los datos.

**Responsable del fichero o del tratamiento:** 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 realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

**Fichero no automatizado:** todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

**Soporte:** objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

**Documento:** todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

**Fuentes accesibles al público (Artículo 7)**

El censo promocional.

Las guías telefónicas.

Las guías profesionales (colegios profesionales)

El censo promocional.

Los diarios y boletines oficiales

Los medios de comunicación social

Las guías de servicio de comunicaciones electrónicas.

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

#### CONTENIDOS DESTACADOS:

Ámbito de aplicación 1

Definiciones 1

Comparativa de los reglamentos 2

Encargado de tratamiento 3

Documento de Seguridad 3

Gestión de soportes 4

Gestión de documentación 4

### ÁMBITO OBJETIVO DE APLICACIÓN

**Se aplicará** a los datos de carácter personal registrados en soporte físico, susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados.

**No se aplicará:**

Al tratamiento de datos que se refieran a personas jurídicas.

A los ficheros que se limiten a incorporar datos de las personas físicas que presten sus servicios en aquéllas.

Datos relativos a empresarios individuales cuando haga referencia a ellos en su calidad de comerciantes, industriales o naveros

Datos de carácter personal de personas fallecidas, aunque las personas vinculadas al fallecido podrán dirigirse a los responsables del fichero que contenga datos del éste para notificar en óbito, o solicitar la cancelación de los datos.

A los ficheros realizados por personas físicas en actividades exclusivamente personales o domésticas. Se considerarán relacionados con éstas, los tratamientos relativos a actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

## COMPARATIVA

RD 994/1999

RD 1720/2007

<p><b>Accesos autorizados:</b> Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.</p> <p><b>Autenticación:</b> Procedimiento de comprobación de la identidad de un usuario.</p> <p><b>Contraseña:</b> información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario</p>	<p><b>Accesos autorizados:</b> autorizaciones concedidas a un usuario para la utilización de los diversos recursos. <u>En su caso, incluirán las autorizaciones o funciones que tengan atribuidas un usuario por delegación del responsable del fichero o tratamiento o responsable de seguridad.</u></p> <p><b>Autenticación :</b> Procedimiento de comprobación de la identidad de un usuario.</p> <p><b>Contraseña:</b> información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o <u>en el acceso a un recurso</u></p>
<p><b>Control de acceso:</b> mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.</p> <p><b>Copia de respaldo:</b> copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.</p> <p><b>Identificación:</b> procedimiento de reconocimiento de la identidad de un usuario.</p> <p><b>Incidencia:</b> cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.</p> <p><b>Recurso:</b> Cualquier parte componente de un sistema de información</p>	<p><b>Control de acceso:</b> mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.</p> <p><b>Copia de respaldo:</b> copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.</p> <p><b>Identificación:</b> procedimiento de reconocimiento de la identidad de un usuario.</p> <p><b>Incidencia:</b> cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.</p> <p><b>Recurso:</b> Cualquier parte componente de un sistema de información</p>
<p><b>Responsable de seguridad:</b> persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.</p> <p><b>Sistema de información:</b> conjunto de ficheros <u>automatizados</u>, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.</p> <p><b>Soporte:</b> objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.</p>	<p><b>Responsable de seguridad:</b> persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.</p> <p><b>Sistema de información:</b> conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.</p> <p><b>Soporte:</b> objeto físico <u>que almacena o contiene datos o documentos, u objeto</u> susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.</p>
<p><b>Usuario:</b> sujeto o proceso autorizado para acceder a datos o recursos.</p>	<p><b>Usuario:</b> Sujeto o proceso autorizado para acceder a datos o recursos. <u>Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario.</u></p>

## NIVELES DE SEGURIDAD

**BASICO:** Todos los ficheros o tratamientos de datos de carácter personal.

**MEDIO:**

- Los relativos a comisión de infracciones administrativas o penales
- Aquellos cuyo funcionamiento se rija por el artículo 29 de la LOPD.
- Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
- Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con prestación de servicios financieros.
- Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social. De igual modo, aquellos de los que sean responsables la mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Aquellos que tengan un conjunto de datos de carácter personal que ofrezcan una definición de las características

o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

**ALTO:**

- Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- Aquellos que contengan datos derivados de actos de violencia de género

**EXCEPCIONES:**

Se aplican medidas de seguridad de nivel básico y medio y la medida de seguridad de nivel alto, relativa al registro de accesos, a los ficheros de los que sean responsables:

- Los operadores que presten servicios de comunicaciones electrónicas disponibles al público o,

- Exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización,

En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
- Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoría se contenga aquellos datos sin guardar relación con su finalidad.
- Se trate de ficheros cuyo único dato de salud haga referencia exclusivamente al grado de discapacidad.
- La simple declaración de la condición de discapacidad o invalidez del afectado con motivo del cumplimiento de deberes públicos.

**EI ENCARGADO DEL TRATAMIENTO** (Artículo 82)**Cuando presta sus servicios en los locales del responsable del fichero :**

Si el responsable del fichero le facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a hacerse constar en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando en dicho acceso se ha prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

**Cuando presta sus servicios en sus propios locales:**

Deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o

Completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad exigibles según la normativa de protección de datos de carácter personal

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento es necesaria una autorización previa del responsable del fichero o tratamiento, y deberá garantizarse el nivel de seguridad correspondiente.

La autorización anterior tendrá que constar en el documento de seguridad y se establecerá un período de validez para un usuario o para un perfil de usuarios

Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener: (art.88)

- La identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo.
- La identificación del responsable.

El período de vigencia del encargo.

El responsable del fichero deberá anotar en su documento de seguridad los casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad , salvo en los datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al documento de seguridad del encargado.

**PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS PERSONALES** (Artículo 83)

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal:

- a datos personales
- a los soportes que los contengan
- a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá :

- la prohibición de acceder a los datos personales
- la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

**DOCUMENTO DE SEGURIDAD**

El Documento de Seguridad deberá estar 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.

Estarán claramente definidas y documentadas en el documento de seguridad:

- Las funciones y obligaciones de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información
- Las funciones de control
- Autorizaciones delegadas por el responsable del fichero o tratamiento.

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.

Los soportes y documentos que contengan datos de carácter personal deberán:

- Permitir identificar el tipo de información que contienen
- Ser inventariados

Solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

En el traslado de la documentación se adoptarán las medidas necesarias para evitar:

- La sustracción
- Pérdida

Acceso indebido a la información durante su transporte.

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá:

- Procederse a su destrucción

Procederse borrado

Para ello se adoptarán medidas dirigidas a evitar:

- El acceso a la información contenida en el mismo
- Su recuperación posterior.

El documento de seguridad establecerá la periodicidad, que no será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Además el Documento de Seguridad contendrá el modo de realización, como mínimo semanal, de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

El responsable del fichero verificará cada seis meses la correcta definición, funcionamiento, aplicación de los procedimientos de copias de respaldo.

A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento se someterán a una auditoría bianual. Así mismo se realizará auditoría cuando se realicen grandes modificaciones.

# Datos al día

Boletín de actualidad  
jurídica en protección  
de datos

Edita: Datalawyers, S.L. protección de datos

Depósito Legal: OU-26/2007

ISSN: 1887-8075

Dirección: Monte dos Postes, 4 bajo derecha  
15703 Santiago de Compostela

Teléfono: 902 367 362

Fax: 981576857

Correo: [datosaldia@datalawyers.com](mailto:datosaldia@datalawyers.com)

Periodicidad trimestral.

Tirada: 500 ejemplares.

Distribución gratuita

Se prohíbe la reproducción total o parcial del contenido de la presente publicación sin autorización de la firma editora.

[www.datalawyers.com](http://www.datalawyers.com)

Consultores de Protección de Datos

## COPIAS DE SEGURIDAD

Se conservará en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá:

Cumplir las medidas de seguridad o utilizar elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

## ACCESO A LOS SISTEMAS DE INFORMACIÓN

El registro de accesos, deberá conservarse durante 2 años cuando el responsable del fichero o del tratamiento :  
Sea una persona física y garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de estas dos circunstancias deberá hacerse constar expresamente en el documento de seguridad.

## CRITERIOS DE ARCHIVO (Artículo 106)

Los criterios previstos para el archivo de los soportes o documentos deberán garantizar:

- la correcta conservación de los documentos
  - la localización Y consulta de la información
- posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

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

## DISPOSITIVOS DE ALMACENAMIENTO (Artículo 107)

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán:

- Disponer de mecanismos que obstaculicen su apertura
- Si no es posible, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

## GESTIÓN DE SOPORTES Y DOCUMENTOS. (Artículo 97)

Deberá establecerse un sistema de registro de entrada de soportes que permita 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 y la forma de envío. La persona responsable de la recepción que deberá estar debidamente autorizada.

## GESTIÓN Y DISTRIBUCIÓN DE SOPORTES. (Artículo 101)

La identificación de los soportes se realizará utilizando sistemas de etiquetado que permitan a los usuarios con acceso autorizado identificar su contenido, y que dificulten la identificación para el resto de personas:

Los sistemas de etiquetado deberán ser:

- Comprensibles y con significado

La distribución de los soportes que contengan datos de carácter personal se realizará :

- Cifrando dichos datos

Utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

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

Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. Cuando sea necesario:

- Se hará constar motivadamente en el documento de seguridad

Se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

## CUSTODIA DE LOS SOPORTES (Artículo 108)

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

## ALMACENAMIENTO DE LA INFORMACIÓN. (Artículo 111)

Los elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse:

En áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante: -llave -otro dispositivo equivalente.

Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

Si ello no fuera posible el responsable adoptará medidas alternativas que se incluirán en el documento de seguridad.

## COPIA O REPRODUCCIÓN. (Artículo 112)

Únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad:

- La generación de copias
- La reproducción de los documentos

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.

## ACCESO A LA DOCUMENTACIÓN. (Artículo 113)

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.

## TRASLADO DE DOCUMENTACIÓN. (Artículo 114)

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a:

- A impedir el acceso
- A impedir la manipulación de la información objeto de traslado.