MATERIAL EXTRA

- **Guía de protección de datos**
- **Guía de seguridad de datos 2008**
- **Tríptico LSSI**
- **Ley Orgánica de Protección de Datos 15/1999**
- **Ley de servicios de la sociedad de la información y de comercio electrónico 34/2002**

Guía de protección de datos:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

by: Levis

Guía

DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

D.L: M-23625-2005
NIPO: 052-04-002-2

Diseño Gráfico: ÉN

Imprime: NILO Industria Gráfica, S.A.

El derecho fundamental a la protección de datos personales deriva directamente de la Constitución y atribuye a los ciudadanos un poder de disposición sobre sus datos, de modo que, en base a su consentimiento, puedan disponer de los mismos.

La Constitución Europea reconoce en dos ocasiones el derecho fundamental a la protección de datos.

Asimismo establece que todos los países miembros de la Unión Europea deberán contar con una autoridad independiente que garantice y tutele tal derecho.

La Ley Orgánica 15/1999 regula el derecho fundamental a la protección de datos y dispone que será la Agencia Española de Protección de Datos la encargada de tutelar y garantizar el derecho.

En el empeño de facilitar un mejor respeto a la protección de datos y divulgar todo lo posible su conocimiento en el marco de una sociedad abierta y democrática, se ha elaborado esta Guía que tengo el gusto de presentar y que, con un lenguaje sencillo y directo, pretende dar un paso más en la necesaria normalización de la cultura de la protección de datos entre los ciudadanos y los responsables de los tratamientos y bases de datos.

Guía

José Luis Piñar Mañas
Director de la Agencia Española de Protección de Datos

Índice

Guía

Los datos personales permiten identificar a una persona.

El nombre, los apellidos, la fecha de nacimiento, la dirección postal o la dirección de correo electrónico, el número de teléfono, el número de identificación fiscal, el número de matrícula del coche, la huella digital, el ADN, una fotografía, el número de seguridad social, ... son datos que identifican a una persona, ya sea directa o indirectamente.

Es habitual que prácticamente para cualquier actividad sea necesario que los datos personales se recojan y utilicen en la vida cotidiana.

Una persona facilita sus datos personales cuando abre una cuenta en el banco, cuando se matricula en un curso de idiomas, cuando se apunta al gimnasio, cuando solicita participar en un concurso, cuando reserva un vuelo o un hotel, cuando pide hora para una consulta médica, cuando busca trabajo, cada vez que efectúa un pago con su tarjeta de crédito, cuando navega por Internet ..... Son múltiples los rastros de datos que se dejan a menudo en todas estas gestiones.

Los mecanismos de recogida y tratamientos de los datos personales se encuentran en constante evolución.

Ello supone que el desarrollo y la aplicación de las nuevas tecnologías ha introducido comodidad y rapidez en el intercambio de datos, lo que ha contribuido también al incremento del número de tratamientos de datos que se realizan cotidianamente. La bondad que aportan estas técnicas es indudable respecto del progreso de las sociedades modernas y de la calidad de vida de los ciudadanos, pero se hace necesario garantizar el equilibrio entre modernización y garantía de los derechos de los ciudadanos.

> Esta ponderación entre derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la Información, es el contexto en el que el Legislador consagra el derecho fundamental a la protección de datos de carácter personal.

¿QUÉ ES EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS?

> El derecho fundamental a la protección de datos reconoce al ciudadano la **facultad de controlar** sus datos personales y la **capacidad para disponer y decidir** sobre los mismos.

La **Constitución Española** en su **artículo 10** reconoce el derecho a la dignidad de la persona. Por su parte, el artículo **18.4** dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

De ambos preceptos deriva el derecho fundamental a la protección de datos de carácter personal, que ha sido definido como autónomo e independiente por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

En desarrollo del citado artículo 18.4, fue aprobada la **Ley Orgánica 15/1999,** de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

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

La LOPD garantiza al ordenamiento jurídico español la **Directiva 95/46/CE (Directiva sobre protección de datos**).

La LOPD garantiza una serie de derechos a las personas físicas, titulares de los datos, tales como el derecho a ser informado de cuándo y porqué se tratan sus datos personales, el derecho a acceder a los datos y, en caso necesario, el derecho a la modificación o supresión de los datos o el derecho a la oposición al tratamiento de los mismos.

El derecho a la protección de datos es un derecho en constante **evolución** que se ha visto reconocido en el **Tratado Europeo por el que se establece una Constitución para Europa.**

La Constitución Europea ha recogido expresamente el derecho fundamental a la protección de datos en dos ocasiones, en la Parte I, Título VI (De la vida democrática de la Unión), el artículo I-51 (Protección de datos de carácter personal) establece en el epígrafe primero que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan" y en la Parte II (Carta de los Derechos Fundamentales de la Unión), Título II (Libertades), se introduce en el artículo II-68 la segunda referencia al derecho a la protección de datos, señalando de nuevo que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan", y añadiendo que "estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley", y que "toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación".

Asimismo, en ambos preceptos se establece que una autoridad independiente se encargará de la garantía del derecho fundamental a la protección de datos personales.

> La Constitución Europea exige que en todos los Estados miembros exista una autoridad independiente que controle y garantice el Derecho Fundamental a la protección de datos.

La Agencia Española de Protección de Datos (en lo sucesivo AEPD) es el ente de derecho público que vela por el cumplimiento de la normativa sobre protección de datos personales, actuando para ello con plena independencia de las Administraciones Públicas.

En este sentido:

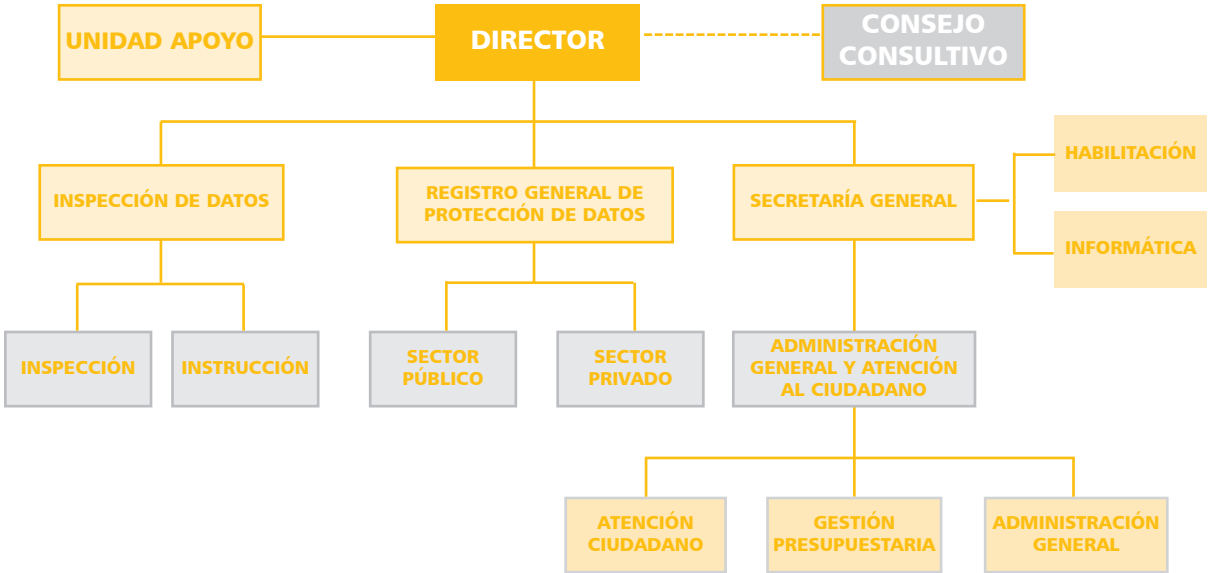
INFORMA sobre el contenido, los principios y las garantías del derecho fundamental a la protección de datos regulado en la LOPD.

AYUDA al ciudadano a ejercitar sus derechos y a los responsables y encargados de tratamientos a cumplir las obligaciones que establece la LOPD.

TUTELA al ciudadano en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido adecuadamente atendidos por los responsables de los ficheros.

GARANTIZA el derecho a la protección de datos investigando aquellas actuaciones de los responsables o encargados de ficheros que puedan ser contrarias a los principios y garantías contenidos en la LOPD. Impone, en su caso, la correspondiente sanción.

La estructura orgánica de la AEPD es la siguiente:



Los datos personales de un ciudadano sólo pueden tratarse, es decir, recogerse y emplearse, si:

El interesado ha dado su consentimiento.

El tratamiento es necesario para el mantenimiento o cumplimiento de un contrato o precontrato de una relación negocial, laboral o administrativa.

El tratamiento es necesario para proteger un interés vital del interesado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

El tratamiento es necesario para cumplir las funciones de las Administraciones Públicas en el ámbito de sus competencias.

Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo del responsable del fichero o de un tercero a quienes se comuniquen los datos.

Cuando una ley habilite el tratamiento sin requerir el consentimiento inequívoco de su titular.

PRINCIPIOS DE PROTECCIÓN DE DATOS

El tratamiento de datos de carácter personal ha de realizarse de acuerdo con los principios de información, calidad, finalidad, consentimiento y seguridad. Dichos principios se plasman en diversos preceptos de la LOPD.

Todo responsable de un fichero o tratamiento de datos personales está obligado a cumplir los citados principios recogidos en la LOPD.

> El responsable de un fichero o tratamiento es la entidad, la persona o el órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales.

Una empresa será la responsable de los ficheros de sus clientes, de sus proveedores, de sus empleados; un médico será responsable del tratamiento de los datos personales que conforman las historias clínicas de sus pacientes; un hotel será responsable del fichero de sus huéspedes; un gimnasio será responsable del fichero de sus socios; un centro educativo será responsable del fichero de sus alumnos; ...

Los principios de la LOPD pretenden proteger los datos personales de los interesados:

Los datos deben tratarse de manera leal y lícita.

Los datos deben recogerse con fines determinados, explícitos y legítimos. Los datos deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y los fines para los que se han recogido.

Los datos deben ser exactos y mantenerse actualizados de manera que respondan con veracidad a la situación actual de su titular.

Los responsables deben atender a los interesados que soliciten el acceso a sus datos personales.

Los datos personales sólo deben conservarse durante el tiempo necesario para las finalidades del tratamiento para el que han sido recogidos. Deben ser cancelados cuando hayan dejado de ser necesarios o pertinentes para el fin con que se obtuvieron.

Todo responsable o encargado de un tratamiento tiene que adoptar todas las medidas necesarias para garantizar la seguridad de los datos personales e impedir cualquier alteración, pérdida, tratamiento o acceso no autorizado.

El responsable tiene que notificar al Registro General de Protección de Datos la creación, modificación o supresión de cualquier fichero o tratamiento de datos personales.

DATOS SENSIBLES

> Se consideran datos sensibles aquellos datos referidos a ideología, creencias, religión, afiliación sindical, salud, origen racial o vida sexual de las personas.

Como norma general los datos de ideología, creencias, religión o afiliación sindical no pueden ser tratados ni almacenados en ficheros. Sólo pueden ser objeto de tratamiento con el consentimiento expreso y por escrito del afectado.

Los datos relativos al origen racial, a la salud y a la vida sexual sólo podrán ser recogidos, tratados y cedidos, si alguna Ley así lo dispone por razones de interés general, o en caso de que el afectado haya consentido expresamente.

Los datos sensibles pueden ser objeto de tratamiento, si resulta necesario para la prevención o para el diagnóstico médicos, para la prestación de asistencia sanitaria o de un tratamiento médicos o para la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario.

También pueden ser tratados estos datos cuando sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para prestar su consentimiento.

Los profesionales sanitarios correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que acuden a los centros sanitarios públicos o privados, de acuerdo con la legislación sanitaria, y guardando el deber de secreto, obligación que subsistirá aún después de finalizar su relación asistencial.

Toda persona tiene derecho a saber porqué y cómo son tratados sus datos personales y decidir acerca del tratamiento

El derecho a la protección de datos puede considerarse una condición preventiva para la garantía de otras libertades y derechos fundamentales.

La LOPD reconoce específicamente a los ciudadanos los siguientes derechos en materia de protección de datos:

DERECHO DE **INFORMACIÓN EN LA RECOGIDA DE DATOS**

DERECHO DE **CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS**

DERECHO DE ACCESO

DERECHO DE **RECTIFICACIÓN**

DERECHO DE CANCELACIÓN

DERECHO DE **OPOSICIÓN**

El ciudadano tiene **derecho a ser informado**, en el momento que facilita sus datos personales.

El **derecho de consulta** permite al ciudadano, dirigiéndose al Registro General de Protección de Datos de la AEPD, conocer de la existencia de un fichero o tratamiento de datos.

El ciudadano puede ejercitar los **derechos de acceso, rectificación, cancelación y oposición** ante el responsable de un fichero o de un tratamiento con el fin de conocer sus datos personales, para solicitar que sean modificados o cancelados, o bien para oponerse a su tratamiento

> Tales derechos pueden ejercerse respecto de cualquier fichero o tratamiento de datos personales, ya sean automatizados o no automatizados

Los derechos de acceso, rectificación, cancelación y oposición tienen carácter personalísimo, es decir, sólo pueden ejercerse por el titular de los mismos o por su representante legal. No obstante, podrá encomendarse su ejercicio a un representante, siempre que el mismo pueda acreditar suficientemente tal condición.

> Todos estos derechos tienen **carácter gratuito**

Estos derechos deben ser respetados por los responsables de los tratamientos de datos personales.

> Si un ciudadano ejercita estos derechos y no recibe, a su juicio, la contestación adecuada puede dirigirse a la Agencia Española de Protección de Datos para solicitar la tutela de estos derechos, para lo cual se instruirá el correspondiente procedimiento.

En la página web de la Agencia **www.agpd.es** se encuentran disponibles los modelos de solicitudes para ejercitar estos derechos, así como para interponer en su caso las relamaciones oportunas ante la propia Agencia.

DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS.
¿Tus datos personales van a ser incluidos en un fichero?
¿Qué tratamientos van a realizarse con tus datos personales?
SÉ CONSCIENTE DE QUE ESTÁS FACILITANDO TUS DATOS PERSONALES.

Cualquier persona tiene derecho a saber si sus datos personales van a ser incluidos en un fichero, y los tratamientos que se realizan con esos datos.

> Los responsables tienen obligación de informar al ciudadano cuando recojan datos personales que le afecten.

El ciudadano debe ser informado de la recogida de sus datos y de su utilización. Este derecho de información es esencial porque condiciona el ejercicio de otros derechos tales como el derecho de acceso, rectificación, cancelación y oposición.

El art. 5 de la LOPD recoge la obligación que tienen los responsables de ficheros o tratamientos de informar a los ciudadanos de la incorporación de sus datos a un fichero, de la identidad y dirección del responsable, de la finalidad del fichero, de los destinatarios de la información, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

En el caso de utilizar Internet como medio de recogida de los datos, también debe facilitarse esta información a los usuarios que registran sus datos.

> Cuando los datos se recojan directamente de los afectados, la información deberá facilitarse con **carácter previo a la recogida de los datos personales.**

Esta obligación general del responsable debe ser facilitada con carácter general, salvo que la información se deduzca inequívocamente de la naturaleza de los propios datos personales y de las circunstancias en las que se produce la recogida.

En la medida de lo posible esta información debe estar incluida en los cuestionarios o impresos de recogida de los datos.

> En el caso de que los datos de carácter personal no hubieran sido recabados del interesado, el responsable del fichero o su representante deben informarle de esa recogida en el plazo de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad.

Si está previsto que los datos sean transmitidos a otras personas, la información debe realizarse a lo más tardar en el momento en que se produzca la primera comunicación de los datos.

DERECHO DE CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS. ¿Quién está tratando tus datos personales?

El art. 14 de la LOPD, permite a cualquier ciudadano dirigirse al Registro General de Protección de Datos (en lo sucesivo RGPD) con el fin de obtener información sobre la existencia de tratamientos de datos de carácter personal, de sus finalidades y de la identidad del responsable del mismo. La consulta al RGPD es pública y gratuita, y su objeto es hacer posible a todo ciudadano el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

> La AEPD no dispone de los datos personales de los ciudadanos incluidos en los ficheros declarados, pero sí puede, previa solicitud de la persona afectada o bien de su representante, facilitar la dirección de la oficina o dependencia del responsable del fichero o tratamiento ante la que se pueden ejercer los derechos de acceso, rectificación, cancelación u oposición, siendo el citado responsable quien debe atender la petición efectuada por la persona titular de los datos.

La consulta al RGPD puede realizarse por escrito o a través de la página web de la Agencia **www.agpd.es**, en la que mensualmente se actualiza la información sobre los ficheros y tratamientos inscritos.

DERECHO DE ACCESO

Toda persona tiene derecho a dirigirse al responsable o encargado de un fichero o tratamiento para conocer la totalidad de los datos personales que le afecten y así mismo, recibir una copia inteligible de los mismos, y cualquier información sobre su origen.

Ejerciendo el derecho de acceso, la persona puede informase de las finalidades del tratamiento, del tipo de datos registrados, de su origen, de los destinatarios de los datos y de las posibles transferencias de datos a otros países.

> El ejercicio del derecho de acceso permite controlar la exactitud de los datos, y en caso de ser necesario, hacerlos rectificar o cancelar.

En virtud del derecho de acceso, regulado en el art. 15 de la LOPD, el ciudadano puede solicitar y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, así como la información disponible sobre el origen de dichos datos y de las comunicaciones realizadas o que se prevean realizar.

> Esta información puede obtenerse bien mediante la mera consulta de los datos por medio de su visualización en pantalla, o bien a través de escrito, copia, telecopia o fotocopia, certificada o no, realizada en forma inteligible, sin utilizar claves o códigos que requieran para su comprensión el uso de dispositivos mecánicos específicos.

El derecho de acceso respecto de los tratamiento realizados por una determinada entidad, persona u órgano administrativo, sólo podrá ejercitarse a intervalos no inferiores a doce meses, salvo que el ciudadano acredite un interés legítimo que posibilite su ejercicio con anterioridad al cumplimiento de dicho período.

Para ejercer este derecho el ciudadano tiene que dirigirse al responsable del fichero o tratamiento, aportando fotocopia del DNI o documento que acredite la identidad y sea admitido en Derecho, o en caso de representación, documento acreditativo de la misma, e indicando el domicilio a efectos de notificaciones, la fecha y firma del solicitante. Los ciudadanos deben utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

> El responsable del fichero o tratamiento tiene que resolver la solicitud de acceso en el plazo máximo de un mes a contar desde la fecha en que haya recibido la solicitud. En caso de estimar la solicitud, el acceso debe hacerse efectivo en el plazo de los diez días siguientes a la notificación.

La obligación de contestar a dicha solicitud ha de producirse con independencia de que figuren o no datos personales del ciudadano en sus ficheros. La contestación al derecho de acceso ha de practicarse utilizando cualquier medio que permita acreditar el envío y la recepción de la misma.

Puede denegarse el derecho de acceso si:

> puede suponer un peligro para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.
>
> o en el caso de ficheros de la Hacienda Pública, si este derecho obstaculiza las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

DERECHO DE RECTIFICACIÓN

El artículo 16 de la LOPD, reconoce al ciudadano el derecho a dirigirse al responsable de un fichero o tratamiento para que rectifique sus datos personales.

> Si un ciudadano contrasta que sus datos personales son inexactos tiene derecho a solicitar su rectificación ante el responsable.

La solicitud de rectificación debe indicar el dato que se estima erróneo y la corrección que debe realizarse y debe ir acompañada de la documentación justificativa de la rectificación solicitada.

> Este derecho puede ejercitarse cuando el tratamiento contenga datos inexactos o incompletos.

El responsable del fichero o tratamiento tiene el deber de atender el derecho de rectificación **en el plazo de diez días hábiles.**

Deberá contestar de forma motivada a la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción de su respuesta.

> Si los datos rectificados hubieran sido cedidos previamente a un tercero, el responsable del fichero tiene la obligación de notificar al cesionario la rectificación practicada.

DERECHO DE CANCELACIÓN

Este derecho, regulado en el art. 16 de la LOPD, ofrece al ciudadano la posibilidad de dirigirse al responsable para solicitar la cancelación de sus datos personales.

> Si un ciudadano verifica que sus datos personales son inexactos o se han tratado ilegalmente, tiene derecho a solicitar su supresión.

Este derecho puede ejercerse cuando el tratamiento no se ajuste a lo dispuesto en la LOPD y, en particular, cuando los datos resulten inexactos o incompletos.

En la solicitud de cancelación, el interesado debe indicar la existencia del dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

> La cancelación dará lugar al bloqueo de los datos cuando sea preciso conservar éstos únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, de cara a posibles responsabilidades.

El bloqueo tendrá una duración equivalente al plazo de prescripción de dichas responsabilidades, debiéndose proceder a la total supresión de los datos una vez cumplido el mismo.

El responsable del fichero o tratamiento tiene la obligación de hacer efectivo el derecho de cancelación en el plazo de diez días naturales.

Deberá contestar de forma motivada a la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción de su respuesta.

> Si los datos cancelados hubieran sido cedidos previamente a un tercero, el responsable del fichero deberá notificar al cesionario la cancelación efectuada.

El responsable del fichero o tratamiento podrá denegar la cancelación, tanto en el caso de ficheros privados como públicos, cuando exista un deber legal de conservación de los datos, durante el plazo establecido en cada caso por la legislación aplicable. Asimismo, podrá denegar la cancelación cuando la conservación del dato sea necesaria para el cumplimiento de las obligaciones contractuales que le vinculen con el interesado y justifiquen el tratamiento de los datos y, en todo caso, cuando su cancelación pudiese causar perjuicio al propio ciudadano titular de los mismos o a terceros.

DERECHO DE OPOSICIÓN

Toda persona tiene la posibilidad de oponerse, por un motivo legitimo y fundado, referido a una situación personal concreta, a figurar en un fichero o al tratamiento de sus datos personales, siempre que una ley no disponga lo contrario. En principio, el ciudadano tiene la facultad de disponer y decidir sobre los usos de los datos personales que le conciernen, y por lo tanto, puede oponerse a aparecer en un determinado fichero o a que sus datos sean comunicados a terceros.

> El ciudadano puede oponerse mediante su simple solicitud, a que sus datos sean tratados con fines de publicidad y de prospección comercial

Este derecho de oposición se encuentra regulado en los arts. 6.4, 17 y 30.4 de la LOPD. Se ejercita mediante una solicitud por escrito dirigida al responsable del fichero o tratamiento, en la que se hagan constar los motivos fundados y legítimos relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

El responsable del fichero o tratamiento tiene un plazo máximo de un mes a contar desde la recepción de la petición, para resolver la solicitud de oposición. Si transcurrido este plazo no se ha recibido de forma expresa una respuesta a la petición de acceso, ésta puede entenderse desestimada a los efectos de presentar una reclamación de tutela de derechos ante la AEPD.

> En el caso de que sea procedente acceder a la oposición, el responsable del fichero ha de excluir del tratamiento los datos del ciudadano solicitante.

En relación a los tratamientos de datos con fines de publicidad y de prospección comercial, los ciudadanos pueden ejercer el derecho de oposición y, a su simple solicitud, el responsable ha de dar de baja sus datos personales en el tratamiento, cancelando de este modo las informaciones que figuraban en el mismo.

> El derecho de oposición puede ejercitarse:
>
> cuando no es obligatoria la recogida de los datos
>
> renunciando a otorgar el consentimiento para el tratamiento de datos especialmente protegidos de ideología, religión o creencias
>
> solicitando la eliminación de datos contenidos en ficheros comerciales
>
> señalando, en su caso, con una x la casilla destinada a indicar que no está de acuerdo con la cesión o comercialización de sus datos

Puede ejercerse en el momento de la recogida de la información o posteriormente, dirigiéndose al responsable del fichero.

> El derecho de oposición no puede ejercerse ante muchos ficheros de titularidad pública, como por ejemplo, los de Hacienda Pública, los ficheros policiales, Seguridad Social, ...

¿QUÉ PUEDES HACER EN CASO DE VIOLACIÓN DE TUS DERECHOS?

En caso de sospechar que han sido violados tus derechos en materia de protección de datos, en primer lugar debes intentar determinar la identidad del responsable del tratamiento. Para ello puedes ejercer tu derecho de consulta al Registro General de Protección de Datos, así como los derechos de acceso, rectificación, cancelación y/u oposición, según sea el caso.

Si no obtienes un resultado satisfactorio con este procedimiento puedes acudir a la Agencia Española de Protección de Datos.

> Las actuaciones contrarias al derecho fundamental a la protección de datos de carácter personal pueden ser denunciadas por los ciudadanos ante la AEPD y, en su caso, posteriormente ante la jurisdicción contencioso-administrativa.

Además, si de dichas actuaciones se derivase un perjuicio para los interesados, los mismos podrán reclamar la correspondiente indemnización, bien ante la jurisdicción civil, bien ante el Órgano administrativo responsable, a través, en este caso, del procedimiento establecido al efecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

> Al ponerte en contacto con la AEPD deberás describir el problema con los suficientes pormenores, para ello puedes utilizar los formularios disponibles en la página web de la AEPD www.agpd.es.

TUTELA DE DERECHOS

El derecho a la tutela de derechos de los ciudadanos por parte de la AEPD está reconocido en el art. 18 de la LOPD.

> El procedimiento de tutela tiene por finalidad garantizar el ejercicio efectivo por parte del ciudadano de los derechos de acceso, rectificación, cancelación y oposición.

El ciudadano al que le haya sido denegado el ejercicio de los derechos de acceso, rectificación, cancelación y oposición puede ponerlo en conocimiento de la AEPD, para que ésta constate la procedencia o improcedencia de la denegación.

Para solicitar la tutela de derechos, el ciudadano tiene que presentar en la AEPD un escrito, en el que se expresen con claridad sus datos, el contenido de la reclamación y los preceptos de la LOPD que considere vulnerados.

La Agencia, a continuación, da traslado de la reclamación al responsable del fichero o tratamiento instándole para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

> La AEPD tramitará el correspondiente procedimiento administrativo y resolverá el mismo en el plazo máximo de seis meses, dando traslado de su resolución a las partes.

Los procedimientos de tutela de derechos no tienen carácter sancionador, limitándose a estimar o desestimar las reclamaciones planteadas por los ciudadanos ante la Agencia. Sin embargo, en algunas ocasiones, los hechos constatados en los citados procedimientos pueden dar lugar a la iniciación de procedimientos sancionadores.

> Las resoluciones del Director de la Agencia Española de Protección de Datos son firmes en vía administrativa por lo que contra las mismas sólo se podrá interponer recurso potestativo de reposición, o bien recurso contencioso-administrativo ante la Audiencia Nacional.

PROCEDIMIENTO SANCIONADOR

Los arts. 43 a 49 de la LOPD regulan el procedimiento sancionador que podrá tramitar la AEPD. Este procedimiento se inicia contra los responsables de ficheros cuando existan pruebas razonables de que se ha producido alguna infracción de los principios y garantías contenidos en la LOPD.

El procedimiento sancionador se inicia siempre de oficio mediante acuerdo del Director de la Agencia cuando existan pruebas razonables de que se ha producido alguna infracción de los principios y garantías contenidos en la LOPD.

El régimen sancionador establecido en los arts. 43 y siguientes de la LOPD, articula las infracciones en tres tipos: leves, graves y muy graves.

Normalmente el acuerdo de iniciación se origina como consecuencia de una denuncia realizada por un ciudadano o de un tercero. En otras ocasiones se debe al conocimiento por parte de la AEPD de un hecho presuntamente ilícito, por ejemplo, a través de alguna noticia aparecida en los medios de comunicación social.

> La AEPD investiga la denuncia y puede suspender temporalmente el tratamiento. En caso de concluir que se ha violado la LOPD la Agencia puede ordenar la supresión o destrucción de los datos o prohibir el tratamiento.

CÓDIGOS TIPO

Los responsables de ficheros o tratamientos de datos de carácter personal están obligados a cumplir los principios y las garantías que establece la LOPD. El cumplimiento de estas obligaciones muchas veces redunda en un aumento de calidad en la prestación de sus servicios y ello, en una mejor consideración por parte de las personas con las que mantiene una relación contractual, negocial, laboral, ...

> Un código tipo es un documento de buenas prácticas en la aplicación de los principios y garantías de protección de datos de carácter personal que ha sido adoptado mediante un acuerdo sectorial, un convenio administrativo o una decisión de empresa, por una organización de responsables de ficheros o tratamientos de datos de titularidad pública o privada.

El art. 32 de la LOPD establece que los códigos tipo deberán ser inscritos en el Registro General de Protección de Datos de la AEPD.

El hecho de que un sector de actividad haya elaborado un código tipo y éste haya sido inscrito en el RGPD puede aportar una garantía adicional a la voluntad y el compromiso de la entidad que exhibe dicho Código de conducta, además de una transparencia en el desarrollo de sus tratamientos de datos.

El cumplimiento de la LOPD es obligatorio para todos los responsables de ficheros o tratamientos de datos de carácter personal.

> Un código tipo no garantiza de manera absoluta el cumplimiento de la normativa de protección de datos de carácter personal.

El art. 29 de la LOPD regula los ficheros o tratamientos de datos de carácter personal derivados de la prestación de servicios de información sobre solvencia patrimonial y crédito. A tal efecto, distingue entre los ficheros o tratamientos de prestación de información sobre la solvencia patrimonial y el crédito y los ficheros sobre cumplimiento o incumplimiento de obligaciones dinerarias (generalmente denominados "ficheros de morosos").

FICHEROS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO Y SOBRE CUMPLIMIENTO O INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS: FICHEROS DE MOROSOS

FICHEROS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO

Estos ficheros aparecen regulados en el artículo 29.1 de la LOPD y su régimen es similar al de los restantes ficheros sometidos a la misma. No obstante, se establecen determinadas especialidades en cuanto a la recogida de los datos.

> Los responsables de este tipo de ficheros se encuentran habilitados por la LOPD para realizar tratamientos sobre datos de carácter personal obtenidos bien de los registros y fuentes accesibles al público establecidos al efecto, o bien de informaciones facilitadas por el interesado o con su consentimiento.

A tal fin el art. 3,j) de la LOPD indica que tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos en la normativa específica, las listas de personas pertenecientes a grupos profesionales (únicamente los datos relativos a nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia a grupo), los diarios y boletines oficiales y los medios de comunicación social. Además, en estos casos, será necesario que la consulta de estas fuentes pueda ser realizada por cualquier persona no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

En todo caso, este tipo de ficheros deberán observar las siguientes reglas en el momento de realizar la recogida de los datos:

No deberán incorporarse datos personales que supongan una información sesgada respecto de aquella que ha aparecido publicada.

Los datos han de referirse a una información exacta.

No deberán incorporar aquellas informaciones que por su naturaleza y circunstancias no permitan una identiicación completa del interesado

> Además, el ciudadano tiene derecho a solicitar al responsable del tratamiento que le comunique los datos, así como las evaluaciones y apreciaciones que se hayan comunicado durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado dichos datos.

FICHEROS SOBRE CUMPLIMIENTO O INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS: FICHERO DE MOROSOS

> El artículo 29.2 de la LOPD permite tratar datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por los acreedores o por quien actúe por su cuenta o interés.

Este caso da lugar a los ficheros o tratamientos comunes de solvencia patrimonial y crédito, conocidos popularmente como "ficheros de morosos".

Como en el caso de los ficheros de información sobre la solvencia patrimonial y el crédito, el ciudadano tiene derecho a solicitar al responsable que le comunique los datos, así como las evaluaciones y apreciaciones que se hayan comunicado durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado dichos datos.

> La inclusión de los datos de carácter personal en los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias, sólo podrá efectuarse cuando exista una deuda cierta, vencida y exigible, que haya resultado impagada, y después de que se haya requerido al ciudadano afectado el pago de la deuda por el acreedor.

No podrán ser incluidos en ficheros de esta naturaleza los datos personales de un ciudadano cuando exista un principio de prueba documental que contradiga la existencia de la propia deuda. Del mismo modo, tal circunstancia determinará la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado la inclusión en el fichero.

Los responsables de estos ficheros sólo podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los ciudadanos y que no se refieran, cuando sean adversos, a más de seis años, y siempre que respondan con veracidad y exactitud a la situación actual de éstos.

> En el caso de que el ciudadano incluido en este tipo de fichero haya procedido al pago de la deuda deberá procederse a la cancelación del dato referido al mismo.

Para ello, el acreedor tendrá que comunicar al responsable del fichero común de información de solvencia patrimonial y crédito, en el plazo de una semana, la inexactitud o inexistencia de la deuda. Por lo tanto, si la deuda ya se ha pagado, el acreedor tiene la obligación de informar al responsable del fichero común para que proceda a la rectificación del dato del ciudadano que no responde a su situación actual.

CARACTERÍSTICAS DE ESTOS FICHEROS

COMUNICACIÓN DE INCLUSIÓN

> En todo caso, el responsable de un fichero o tratamiento común de morosidad tiene la obligación de notificar al ciudadano que ha procedido a incluirlo en el mismo haciendo referencia de los datos incluidos, así como al derecho que le asiste para recabar información de la totalidad de ellos en los términos establecidos en la LOPD.

Dicha notificación deberá efectuarse por el responsable en el plazo máximo de treinta días a contar desde el registro del dato, e informará al afectado de su derecho a recabar información sobre los datos recogidos en el mismo.

La inscripción en el fichero o tratamiento común de la obligación incumplida se efectuará, bien en un solo asiento, si fuese de vencimiento único, bien en tantos asientos como vencimientos periódicos incumplidos existan, señalando, en este caso, la fecha concreta de cada uno de ellos.

Se efectuará una notificación por cada deuda concreta y determinada, con independencia de que ésta se tenga con el mismo o con distintos acreedores.

El responsable del fichero común deberá adoptar las medidas organizativas y técnicas necesarias que permitan acreditar la realización material del envío de la comunicación y la fecha de entrega o intento de entrega de la notificación.

> La notificación se dirigirá a la última dirección conocida del afectado, a través de un medio fiable e independiente del responsable del fichero o tratamiento común.

DERECHO DE ACCESO

En relación con este derecho, los responsables de los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito están obligados a satisfacer el derecho de acceso, cualquiera que sea el origen de los datos incluidos en los mismos.

> Además, cuando el ciudadano lo solicite, el responsable del fichero común deberá informar sobre las evaluaciones y apreciaciones que se hayan comunicado en los últimos seis meses, así como el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

Las personas o entidades a las que se presta el servicio solamente están obligadas, ante el ejercicio del derecho de acceso, rectificación y cancelación de un ciudadano, a comunicar los datos relativos al mismo a los que tengan acceso, y la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN

> En los ficheros comunes de prestación de servicios de información sobre solvencia patrimonial y crédito, cuando el afectado lo solicite, el responsable del fichero deberá cumplir la obligación de atender los derechos de rectificación y cancelación.

En relación al ejercicio de estos derechos se pueden plantear los siguientes supuestos:

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige al responsable del fichero común, éste trasladará dicha solicitud al acreedor que haya facilitado los datos relativos a la deuda, para que éste resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte del acreedor en el plazo de diez días, procederá cautelarmente a la rectificación o cancelación de los mismos.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige a otra entidad participante en el sistema y hace referencia a datos que dicha entidad haya facilitado al fichero común, por ser la misma la acreedora del interesado, dicha entidad procederá a la rectificación o cancelación de los datos en sus ficheros y a notificarlo al responsable del fichero común en el plazo de diez días.

Si la solicitud hace referencia a datos que la entidad acreedora no hubiera facilitado al fichero común, dicha entidad informará al afectado sobre este hecho, proporcionándole, además, la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

FICHEROS DE MARKETING Y PUBLICIDAD

> Las entidades que se dedican a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial ... pueden utilizar los nombres y direcciones, así como otros datos personales que figuren en fuentes accesibles al público.

Los repertorios telefónicos y las listas de personas pertenecientes a un Colegio profesional, que contengan los datos de nombre, título, profesión, actividad, grado académico, y la dirección son fuentes de acceso público. También lo son los diarios y boletines oficiales y los medios de comunicación.

Cuando una entidad toma datos personales de una fuente accesible al público para realizar un tratamiento de publicidad o marketing debe informar al interesado del origen de los datos y de la identidad del responsable del tratamiento, diarios y boletines oficiales y medios de comunicación.

Los interesados pueden ejercer el derecho de acceso para conocer sus datos personales y el origen de los mismos.

Toda persona tiene derecho a oponerse al tratamiento de sus datos personales con esta finalidad.

La información de esta guía puede ser ampliada en

www.agpd.es

Servicio de Atención al Ciudadano

Sagasta nº 22. 28004 Madrid
correo - e: ciudadano@agpd.es
tl: 901 100 099 fax: 91 445 56 99

Guía de seguridad de datos 2008

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS
by: Levis

GUíA de Seguridad de Datos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NIPO: 052-08-003-6

Diseño Gráfico: ÉN by: Levis

Imprime: NILO Industria Gráfica, S.A.

GUíA de Seguridad de Datos

índice

INTRODUCCIÓN

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

El Reglamento de desarrollo de la LOPD (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre, fue publicado en el BOE número 17, de 19 de enero de 2008. El Título VIII de este reglamento desarrolla las medidas de seguridad en el tratamiento de datos de carácter personal y tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Entre estas medidas, se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

Con el objeto de facilitar a los responsables de ficheros y a los encargados de tratamientos de datos personales la adopción de las disposiciones del RLOPD, la Agencia Española de Protección de Datos pone a su disposición este documento, en el que se recopila un cuadro resumen de las medidas de seguridad recogidas en el citado Título VIII, un modelo de "Documento de Seguridad", que sirve de guía y facilita el desarrollo y cumplimiento de la normativa sobre protección de datos, y por último, una relación de comprobaciones con el objeto de facilitar la realización de la auditoría de seguridad.

AVISO IMPORTANTE:

Debe entenderse, en cualquier caso, que siempre habrá que atenerse a lo dispuesto en la LOPD, en el RLOPD, y en el resto de previsiones relativas a la protección de datos de carácter personal, y que la utilización de este modelo como guía de ayuda para desarrollar un "Documento de Seguridad" debe, en todo caso, tener en cuenta los aspectos y circunstancias aplicables en cada caso concreto, sin prejuzgar el criterio de la Agencia Española de Protección de Datos en el ejercicio de sus funciones.

En la web de la Agencia Española de Protección de Datos se encuentra disponible la versión actualizada de esta Guía de Seguridad (**www.agpd.es**)

MEDIDAS DE SEGURIDAD

Las medidas de seguridad exigibles a los ficheros y tratamientos de datos personales se clasifican en tres niveles: BÁSICO, MEDIO y ALTO.

APLICACION DE NIVELES

A continuación se indican los ficheros y tratamientos a los que corresponde aplicar las medidas de seguridad relativas a cada uno de los niveles que determina el RLOPD.

NIVEL ALTO. Ficheros o tratamientos con datos:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;
- recabados con fines policiales sin consentimiento de las personas afectadas; y
- derivados de actos de violencia de género.

NIVEL MEDIO. Ficheros o tratamientos con datos:

- relativos a la comisión de infracciones administrativas o penales;
- que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);
- de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;

- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;
- que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y
- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización [1]

NIVEL BÁSICO. Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
- se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero; y
- en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

MEDIDAS A APLICAR

EL DOCUMENTO DE SEGURIDAD

Es un documento interno de la organización, que debe mantenerse siempre actualizado. Disponer del documento de seguridad es una obligación para todos los responsables de ficheros y, en su caso, para los encargados del tratamiento, con independencia del nivel de seguridad que sea necesario aplicar.

Los apartados mínimos que debe incluir el documento de seguridad son los siguientes:

- ámbito de aplicación: especificación detallada de los recursos protegidos;
- medidas, normas, procedimientos, reglas y estándares de seguridad;
- funciones y obligaciones del personal,

1 Para esta categoría de ficheros además deberá disponerse de un registro de accesos

- estructura y descripción de los ficheros y sistemas de información;
- procedimiento de notificación, gestión y respuesta ante incidencias;
- procedimiento de copias de respaldo y recuperación de datos;
- medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.

A partir del nivel medio de medidas de seguridad, además de los apartados anteriores, deberán incluirse los siguientes:

- identificación del responsable de seguridad y
- control periódico del cumplimiento del documento

En caso de haber contratado la prestación de servicios por terceros para determinados ficheros, en el documento de seguridad se debe hacer constar esta circunstancia, indicando una referencia al contrato y su vigencia, así como los ficheros objeto de este tratamiento.

Si se ha contratado la prestación de servicios en relación con la totalidad de los ficheros y tratamientos de datos del responsable, y dichos servicios se prestan en las instalaciones del encargado del tratamiento se podrá delegar en éste la llevanza del documento de seguridad.

En el capítulo de "Guía modelo del Documento de seguridad" se encuentra el modelo que facilita la elaboración de este documento de seguridad.

	Nivel Básico	Nivel Medio	Nivel Alto
RESPONSABLE DE SEGURIDAD		El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.	
PERSONAL	Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. Definición de las funciones de control y las autorizaciones delegadas por el responsable. Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.		
INCIDENCIAS	Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. Procedimiento de notificación y gestión de las incidencias.	SOLO FICHEROS AUTOMATIZADOS Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. Autorización del responsable del fichero para la recuperación de datos.	
CONTROL DE ACCESO	Relación actualizada de usuarios y accesos autorizados. Control de accesos permitidos a cada usuario según las funciones asignadas. Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. Concesión de permisos de acceso sólo por personal autorizado. Mismas condiciones para personal ajeno con acceso a los recursos de datos.	SOLO FICHEROS AUTOMATIZADOS Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	SOLO FICHEROS AUTOMATIZADOS Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. Revisión mensual del registro por el responsable de seguridad. Conservación 2 años. No es necesario este registro si el responsable del fichero es una persona física y es el único usuario. SOLO FICHEROS NO AUTOMATIZADOS Control de accesos autorizados. Identificación accesos para documentos accesibles por múltiples usuarios.

	Nivel Básico	Nivel Medio	Nivel Alto
IDENTIFICACIÓN Y AUTENTICACIÓN	SOLO FICHEROS AUTOMATIZADOS Identificación y autenticación personalizada. Procedimiento de asignación y distribución de contraseñas. Almacenamiento ininteligible de las contraseñas. Periodicidad del cambio de contraseñas (<1 año).	SOLO FICHEROS AUTOMATIZADOS Limite de intentos reiterados de acceso no autorizado.	
GESTIÓN DE SOPORTES	Inventario de soportes. Identificación del tipo de información que contienen, o sistema de etiquetado. Acceso restringido al lugar de almacenamiento. Autorización de las salidas de soportes (incluidas a través de e-mail) Medidas para el transporte y el desecho de soportes.	SOLO FICHEROS AUTOMATIZADOS Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.	SOLO FICHEROS AUTOMATIZADOS Sistema de etiquetado confidencial. Cifrado de datos en la distribución de soportes. Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).
COPIAS DE RESPALDO	SOLO FICHEROS AUTOMATIZADOS Copia de respaldo semanal. Procedimientos de generación de copias de respaldo y recuperación de datos. Verificación semestral de los procedimientos. Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita. Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.		SOLO FICHEROS AUTOMATIZADOS Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
CRITERIOS DE ARCHIVO	SOLO FICHEROS NO AUTOMATIZADOS El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)		

	Nivel Básico	Nivel Medio	Nivel Alto
ALMACENAMIENTO	SOLO FICHEROS NO AUTOMATIZADOS Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.		SOLO FICHEROS NO AUTOMATIZADOS Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave.
CUSTODIA SOPORTES	SOLO FICHEROS NO AUTOMATIZADOS Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.		
COPIA O REPRODUCCIÓN			SOLO FICHEROS NO AUTOMATIZADOS Sólo puede realizarse por los usuarios autorizados. Destrucción de copias desechadas.
AUDITORIA		Al menos cada dos años, interna o externa. Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. Verificación y control de la adecuación de las medidas. Informe de detección de deficiencias y propuestas correctoras. Análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero.	
TELECOMUNICACIONES			SOLO FICHEROS AUTOMATIZADOS Transmisión de datos a través de redes electrónicas cifradas.
TRASLADO DOCUMENTACIÓN			SOLO FICHEROS NO AUTOMATIZADOS Medidas que impidan el acceso o manipulación.

- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.

- La ejecución de trabajos fuera de los locales del responsable o del encargado del tratamiento debe ser previamente autorizada por el responsable del fichero, constar en el documento de seguridad y garantizar el nivel de seguridad.

- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.

- Acceso facilitado a un encargado del tratamiento deberá constar en el documento de seguridad y deberá comprometerse al cumplimiento de las medidas de seguridad previstas.

ORGANIZACIÓN DEL MODELO

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. En este caso se ha optado por el primer tipo, organizando el "documento de seguridad" en dos partes: en la primera se recogen las medidas que afectan a todos los sistemas de información de forma común con independencia del sistema de tratamiento sobre el que se organizan: informatizado, manual o mixto, y en la segunda se incluye un anexo por cada fichero o tratamiento, con las medidas que le afecten de forma concreta. Además, se han especificado aquellas medidas que afectan sólo a ficheros automatizados y las que afectan a los no automatizados de forma exclusiva.

El modelo se ha redactado con el objeto de recopilar las exigencias mínimas establecidas por el Reglamento. Es posible y recomendable incorporar cualquier otra medida que se considere oportuna para aumentar la seguridad de los tratamientos, o incluso, adoptar las medidas exigidas para un nivel de seguridad superior al que por el tipo de información les correspondería, teniendo en cuenta la infraestructura y las circunstancias particulares de la organización.

Dentro del modelo se utilizarán los siguientes símbolos convencionales:
<comentario explicativo>: Entre los caracteres "<" y ">", se encuentran los comentarios aclaratorios sobre el contenido que debe tener un campo. Estos textos no deben figurar en el documento final, y deben desarrollarse para ser aplicados a cada caso concreto.

NIVEL MEDIO: con esta marca se señalarán las medidas que sólo son obligatorias en los ficheros que tengan que adoptar un nivel de seguridad medio.

NIVEL ALTO: Con esta marca se señalarán las medidas que sólo son obligatorias en los ficheros que tengan que adoptar un nivel de seguridad alto.

A: Con esta marca se señalarán las medidas específicas para aplicar exclusivamente a ficheros informatizados o automatizados.

M: Con esta marca se señalarán las medidas específicas para aplicar exclusivamente a ficheros manuales o no automatizados.

Las medidas que no van precedidas de ninguna de estas marcas deben aplicarse con carácter general, tanto a ficheros o tratamientos automatizados como no automatizados y con independencia del nivel de seguridad.

NOTA ACLARATORIA: Las medidas de seguridad de nivel básico son exigibles en todos los casos. Las medidas de nivel medio complementan a las anteriores en el caso de ficheros clasificados en este nivel, y las de nivel alto, cuando deban adoptarse, incluyen también las de nivel básico y medio.

DOCUMENTO DE SEGURIDAD

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el RLOPD recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la LOPD.

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.

- Procedimiento general de información al personal.
- Funciones y obligaciones del personal.
- Procedimientos de notificación, gestión y respuestas ante las incidencias.
- Procedimientos de revisión.
- Consecuencias del incumplimiento del Documento de Seguridad.

ANEXO I. Descripción de ficheros.

ANEXO II. Nombramientos.

ANEXO III. Autorizaciones de salida o recuperación de datos.

ANEXO IV. Delegación de autorizaciones.

ANEXO V. Inventario de soportes.

ANEXO VI. Registro de incidencias.

ANEXO VII. Encargados de tratamiento.

ANEXO VIII. Registro de entrada y salida de soportes.

ANEXO IX. Medidas alternativas.

ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente 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.

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

NIVEL ALTO: Se aplicarán a los ficheros o tratamientos de datos:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;
- recabados con fines policiales sin consentimiento de las personas afectadas; y
- derivados de actos de violencia de género.

NIVEL MEDIO: Se aplicarán a los ficheros o tratamientos de datos:

- relativos a la comisión de infracciones administrativas o penales;
- que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);
- de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;
- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;
- que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y

- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización[2].

NIVEL BÁSICO: Se aplicarán a cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
- se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero; y
- en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

<incluir relación de ficheros o tratamientos afectados, indicando si se trata de sistemas automatizados, manuales o mixtos, y el nivel de seguridad que les corresponde>.
.....
.....
En el Anexo I se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

2 Para esta categoría de ficheros además deberá disponerse de un registro de accesos.

MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

IDENTIFICACIÓN Y AUTENTICACIÓN

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

A

- <Especificar las normativas de identificación y autenticación de los usuarios con acceso a los datos personales. La identificación de los usuarios se deberá realizar de forma inequívoca y personalizada, verificando su autorización (cada identificación debe pertenecer a un único usuario).

- Si la autenticación se realiza mediante contraseñas, detallar el procedimiento de asignación, distribución y almacenamiento que deberá garantizar su confidencialidad e integridad, e indicar la periodicidad con la que se deberán cambiar, en ningún caso superior a un año.

- También es conveniente incluir los requisitos que deben cumplir las cadenas utilizadas como contraseña>.

A

NIVEL MEDIO En los ficheros <indicar los nombres de los ficheros de nivel medio y alto>, se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

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 <incluir estos mecanismos>.

Exclusivamente el <persona autorizada (o denominación de su puesto de trabajo) para conceder, alterar o anular el acceso autorizado> está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del fichero <nota: si la persona es diferente en función del fichero, incluir el párrafo en la parte del Anexo I correspondiente>.

<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.

Incluir y detallar los controles de acceso a los sistemas de información>.

En el Anexo I, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista se actualizará <Especificar procedimiento de actualización>.

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.

NIVEL ALTO: REGISTRO DE ACCESOS

A

En los accesos a los datos de los ficheros de nivel alto, <indicar los nombres 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.

<Indicar si se estima oportuno, información relativa al sistema de registro de accesos. 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 conservaran durante <especificar periodo, que deberá ser al menos de dos años. No es preciso que estos datos se almacenen "on-line">.

El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe según se detalla en el capítulo de "Comprobaciones para la realización de la auditoría de seguridad" de este documento.

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, y
- se haga constar en el documento de seguridad.

M

El acceso a la documentación se limita exclusivamente al personal autorizado.
Se establece el siguiente mecanismo para identificar los accesos realizados en el caso de los documentos relacionados <indicar los documentos o tipos de documentos que puedan ser utilizados por múltiples usuarios, así como el mecanismo establecido para controlar estos accesos; igualmente se definirá en este punto un registro de accesos general>.

GESTIÓN DE SOPORTES Y DOCUMENTOS

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en <indicar el lugar de acceso restringido donde se almacenarán>, lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación: <especificar el personal autorizado a acceder al lugar donde se almacenan los soportes que contengan datos de carácter personal, el procedimiento establecido para habilitar o retirar el permiso de acceso. Tener en cuenta el procedimiento a seguir para casos en que personal no autorizado tenga que tener acceso a los locales por razones de urgencia o fuerza mayor>.

Los siguientes soportes <relacionar aquellos a que se refiere> cumplirán con las obligaciones indicadas en el párrafo anterior, dadas sus características físicas, que imposibilitan el cumplimiento de las mismas.

Los siguientes soportes <indicar aquellos que contengan datos considerados especialmente sensibles y respecto de los que se haya optado por proceder del siguiente modo> se identificarán utilizando los sistemas de etiquetado siguientes <especificar los criterios de etiquetado que serán comprensibles y con significado para los usuarios autorizados, permitiéndoles identificar su contenido, y que sin embargo dificultarán la identificación para el resto de personas>.

Los soportes se almacenarán de acuerdo a las siguientes normas: <indicar normas de etiquetado de los soportes. Especificar el procedimiento de inventariado y almacenamiento de los mismos. El inventario de soportes puede anexarse al documento o gestionarse de forma automatizada, en este último caso se indicará en este punto el sistema informático utilizado>.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos, fuera de los locales bajo el control del responsable del tratamiento, deberá ser autorizada por el responsable del fichero o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento <detallar el procedimiento a

seguir para que se lleve a cabo la autorización. Tener en cuenta también los ordenadores portátiles y el resto de dispositivos móviles que puedan contener datos personales>.

En el Anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

Los soportes que vayan a ser desechados, deberán ser previamente <detallar procedimiento a realizar para su destrucción o borrado> de forma que no sea posible el acceso a la información contenida en ellos o su recuperación posterior.

En el traslado de la documentación se adoptarán las <indicar medidas y procedimientos previstos> para evitar la sustracción, pérdida o acceso indebido a la información.

A

NIVEL MEDIO : REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

Las salidas y entradas de soportes correspondientes a los ficheros <indicar los nombres de los ficheros de nivel medio y alto>, serán registradas de acuerdo al siguiente procedimiento: <Detallar el procedimiento por el que se registrarán las entradas y salidas de soportes>. El registro de entrada y salida de soportes se gestionará mediante <indicar la forma en que se almacenará el registro, que puede ser manual o informático> y en el que deberán constar <indicar los campos del registro, que deberán ser, al menos, en el caso de las entradas, 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 autorizada responsable de la recepción; y en el caso de las salidas, 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 autorizada responsable de la entrega>.

<En caso de gestión automatizada se indicará en este punto el sistema informático utilizado>.

A

NIVEL ALTO: GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

Los soportes relacionados <indicar aquellos de nivel alto> se identificarán mediante el sistema de etiquetado <especificar los criterios de etiquetado que resultarán comprensibles y con significado para los usuarios con acceso autorizados, permitiéndoles identificar su contenido y dificultando la identificación para el resto de personas>.

La distribución y salida de soportes que contengan datos de carácter personal de los ficheros <indicar los nombres de los ficheros de nivel alto> se realizará <indicar el procedimiento para cifrar los datos o, en su caso, para utilizar el mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte. Igualmente se cifrarán los datos que contengan los dispositivos portátiles cuando se encuentren fuera de las instalaciones que están bajo control del responsable>.

Los siguientes dispositivos portátiles <relacionar aquellos que no permitan el cifrado de los datos personales>, debido a las razones indicadas <motivar la necesidad de hacer uso de este tipo de dispositivos>, se utilizarán en el tratamiento de datos personales adoptándose las medidas que a continuación se explicitan <relacionar las medidas alternativas que tendrán en cuenta los riesgos de realizar tratamientos en entornos desprotegidos>.

M

CRITERIOS DE ARCHIVO

El archivo de los soportes o documentos se realizará de acuerdo con los criterios <indicar los previstos en la legislación que les afecte o en su defecto, los establecidos por el responsable del fichero, que en cualquier caso garantizarán la correcta conservación de los documentos, la localización y consulta de la información y posibilitarán el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación>.

M

ALMACENAMIENTO DE LA INFORMACIÓN

Los siguientes dispositivos <relacionarlos así como aquellas de sus características que obstaculicen su apertura. Cuando sus características físicas no permitan adoptar esta medida, el responsable adoptará medidas que impidan el acceso a la información de personas no autorizadas> se utilizarán para guardar los documentos con datos personales.

NIVEL ALTO: Los elementos de almacenamiento <indicar tipos como armarios, archivadores u otros elementos utilizados> respecto de los documentos con datos personales, se encuentran en <indicar lugares físicos y protección con que cuenta el acceso a las mismas, como llaves u otros dispositivos. Además estos lugares permanecerán cerrados en tanto no sea preciso el acceso a los documentos. Si a la vista de las características de los locales no fuera posible cumplir lo anteriormente indicado, se adoptarán medidas alternativas que se reflejarán en este punto>.

M

CUSTODIA DE SOPORTES

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamientos indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas.

ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

<Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones, sean o no públicas, garantizarán un nivel de seguridad equivalente al exigido para los accesos en modo local. Relacionar los accesos previstos y los ficheros a los que se prevea acceder>.

A

NIVEL ALTO: Los datos personales correspondientes a los ficheros <relacionar los de nivel alto>, que se transmitan a través de redes públicas o inalámbricas de comunicaciones electrónicas se realizará cifrando previamente estos datos <indicar en su caso otros mecanismos distintos del cifrado que se utilicen y que garanticen que la información no sea inteligible ni manipulada por terceros. También es adecuado cifrar los datos en red local>.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

Se pueden llevar a cabo los siguientes tratamientos de datos personales <relacionar los ficheros a que afecten estos tratamientos> fuera de los locales del responsable del fichero <indicar en su caso, los distintos locales a los que deban circunscribirse, especialmente en el supuesto de que se realicen tratamientos por un encargado del tratamiento que se especificará>, así como mediante dispositivos portátiles. Esta autorización regirá durante <indicar el período de validez de la misma>.

<Esta autorización puede realizarse para unos usuarios concretos que hay que indicar o para un perfil de usuarios>.

<Se debe garantizar el nivel de seguridad correspondiente>.

M

TRASLADO DE DOCUMENTACIÓN

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse las siguientes medidas <relacionar las medidas necesarias y en su caso alternativas recomendadas, orientadas a impedir el acceso o manipulación de la información objeto de traslado>.

FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

M

NIVEL ALTO

COPIA O REPRODUCCIÓN

La realización de copias o reproducción de los documentos con datos personales sólo se podrán realizar bajo el control del siguiente personal autorizado <indicar los usuarios o perfiles habilitados para ello>.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida <indicar los medios a utilizar o puestos a disposición de los usuarios para ello>.

A

COPIAS DE RESPALDO Y RECUPERACIÓN

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos, con la siguiente periodicidad <especificarla, y en todo caso será como mínimo una vez a la semana>.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente respecto de los ficheros parcialmente automatizados siguientes <indicarlos>, se grabarán manualmente los datos. <Para la grabación manual indicada deberá existir documentación que permita dicha reconstrucción>.

El responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

NIVEL ALTO: En los ficheros <indicar ficheros de nivel alto> se conservará una copia de respaldo y de los procedimientos de recuperación de los datos en <especificar el lugar, diferente de donde se encuentran los sistemas informáticos que los tratan, y que deberá cumplir las medidas de seguridad, o utilizando elementos que garanticen la integridad y recuperación de la información de forma que sea recuperable>.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD

Se designa como responsable de seguridad <indicarlo/s en el caso de que se prevea que sean varios>, que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad. <La designación puede ser única para todos los ficheros o diferenciada según los sistemas de tratamiento, lo que se especificará en este documento, en la parte correspondiente del Anexo I>.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde a <denominación responsable del fichero o del encargado del tratamiento> como responsable del fichero de acuerdo con el RLOPD.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de <indicar periodo de desempeño del cargo>. Una vez transcurrido este plazo <denominación responsable del fichero> podrá nombrar al mismo responsable de seguridad o a otro diferente.

En el Anexo II se encuentran las copias de los nombramientos de responsables de seguridad.

PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el Capítulo siguiente y de forma específica para cada fichero en la parte del Anexo I correspondiente.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento: <indicar el procedimiento por el cual se informará a cada persona, en función de su perfil, de las normas que debe cumplir y de las consecuencias de no hacerlo. Puede ser conveniente incluir algún sistema de acuse de recibo de la información>.

<Si se estima oportuna, la remisión periódica de información sobre seguridad: circulares, recordatorios, nuevas normas, indicar aquí el procedimiento y las personas autorizadas para hacerlo>.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

FUNCIONES Y OBLIGACIONES DE CARÁCTER GENERAL.

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al <responsable del fichero o de seguridad en su caso> las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias".

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Funciones y obligaciones de <incluir un punto con las obligaciones detalladas de los perfiles que afectan a todos los ficheros, como por ejemplo, administradores de los sistemas, responsables de informática, responsable/s de seguridad si existe/n, responsables de seguridad física, etc. Es importante que se concrete la persona o cargo que corresponde a cada perfil. También deben contemplarse los procedimientos de actuación o delegación de funciones para casos de ausencia. Este apartado se propone principalmente como un recopilatorio que agrupe las medidas que en el resto del Documento se asignan a perfiles concretos>.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto de aquellos datos que hubiera podido conocer durante la prestación del servicio.

Se delegan las siguientes autorizaciones en los usuarios relacionados <indicar usuarios, o perfiles y autorizaciones que el responsable del fichero delega en ellos para su ejercicio>.

PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de <denominación del responsable del fichero>.

El procedimiento a seguir para la notificación de incidencias será <especificar concretamente los procedimientos de notificación y gestión de incidencias, indicando quien tiene que notificar la incidencia, a quien y de que modo, así como quien gestionará la incidencia>.

El registro de incidencias se gestionará mediante <indicar la forma en que se almacenará el registro, que puede ser manual o informático, y en el que deberán constar, al menos, el tipo de incidencia, el momento en que se ha producido o en su caso detectado, la persona que realiza la notificación, a quién se comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. En caso de gestión automatizada se indicará en este punto el sistema informático utilizado>.

A

NIVEL MEDIO: En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros <relacionar los ficheros de nivel medio y alto>, del modo que se indica a continuación <detallar el procedimiento para registrar las recuperaciones de datos, que deberá incluir la persona que ejecutó el proceso, los datos restaurados y, en su caso, que datos ha sido necesario grabar manualmente en el proceso de recuperación. En caso de gestión automatizada, se deberá prever la existencia de un código específico para recuperaciones de datos, en la información relativa al tipo de incidencia>.

NIVEL MEDIO: Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del responsable del fichero.

En el Anexo III se incluirán los documentos de autorización del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

PROCEDIMIENTOS DE REVISIÓN

REVISIÓN DEL DOCUMENTO DE SEGURIDAD

<Especificar los procedimientos previstos para la modificación del documento de seguridad, con especificación concreta de las personas que pueden o deben proponerlos y aprobarlos, así como para la comunicación de las modificaciones al personal que pueda verse afectado.

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>.

NIVEL MEDIO: AUDITORÍA

<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, según lo indicado en sus artículos 96 y 110 respecto de ficheros automatizados y no automatizados respectivamente, y que debe realizarse al menos cada dos años.

Con carácter extraordinario deberá realizarse cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas, con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoria inicia el cómputo de dos años señalado.

El informe analizará la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

Los informes de auditoría han de ser analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos, o en su caso de las autoridades de control de las comunidades autónomas>.

NIVEL ALTO: INFORME MENSUAL SOBRE EL REGISTRO DE ACCESOS

<Indicar los procedimientos para realizar el informe mensual sobre el registro de accesos a los datos de nivel alto regulado por el artículo 24 del RLOPD>.

CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a <indicar la normativa sancionadora aplicable>.

ANEXO I
DESCRIPCIÓN DE FICHEROS

Actualizado a: <fecha de la última actualización del anexo>.

<Se incluirá un anexo de este tipo por cada fichero incluido en el ámbito del documento de seguridad, podrían denominarse ANEXO I a, b, c, etc.>.

- Nombre del fichero o tratamiento: <rellenar con nombre del fichero>.
- Unidad/es con acceso al fichero o tratamiento: <especificar departamento o unidad con acceso al fichero, si aporta alguna información>.
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos: <rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)>.
    - □ Identificador: <código de inscripción>.
    - □ Nombre: <nombre inscrito>.
    - □ Descripción: <descripción inscrita>.
- Nivel de medidas de seguridad a adoptar: <básico, medio o alto>.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD

<Persona designada por el responsable del fichero al objeto de coordinar y controlar las medidas incluidas en este documento para este fichero, en el caso de que existan varios, o para todos los ficheros en el supuesto de que se trate de designación única>.

- Administrador: <persona designada para conceder, alterar, o anular el acceso autorizado a los datos>.

- Leyes o regulaciones aplicables que afectan al fichero o tratamiento <si existen>.

- Código Tipo Aplicable: <se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el articulo 32 de la LOPD>.

- Estructura del fichero principal: <incluir los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 81 del Reglamento de desarrollo de la LOPD >.

- 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: <indicar proce dencia de los datos, quién suministra los datos>.
  - □ Procedimiento de recogida: <encuestas, formularios en papel, Internet, ...>.
  - □ Cesiones previstas: <relacionar los destinatarios de los datos previstos>.
  - □ Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>.
  - □ Sistema de tratamiento: <automatizado, manual o mixto>.

- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: <indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>

- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.

- Información sobre conexión con otros sistemas: <Describir las posibles relaciones con otros ficheros del mismo responsable>.

- Funciones del personal con acceso a los datos personales: <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.

- Descripción de los procedimientos de control de acceso e identificación: <Cuando sean específicos para el fichero>.

- Relación actualizada de usuarios con acceso autorizado: <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.

<Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.

ANEXO II
NOMBRAMIENTOS

<Adjuntar original o copia de los nombramientos que afecten a los diferentes perfiles incluidos en este documento, como el del responsable de seguridad>.

ANEXO III
AUTORIZACIONES DE SALIDA O RECUPERACIÓN DE DATOS

<Adjuntar original o copia de las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, así como aquellas relativas a la ejecución de los procedimientos de recuperación de datos>.

ANEXO IV
DELEGACIÓN DE AUTORIZACIONES

En su caso, personas en las que el responsable del fichero ha delegado <Indicar las autorizaciones, tales como: salida de dispositivos portátiles, la copia o reproducción de documentos en soporte papel, …>.

ANEXO V
INVENTARIO DE SOPORTES

<Si el inventario de soportes se gestiona de forma no automatizada recoger en este anexo la información al efecto, según lo indicado en el apartado de "Gestión de soportes y Documentos" de este documento. Los soportes deberán permitir identificar el tipo de información, que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en este documento>.

ANEXO VI
REGISTRO DE INCIDENCIAS

<Si el registro de incidencias se gestiona de forma no automatizada, recoger en este anexo la información al efecto, según lo indicado en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias" de este documento>.

ANEXO VII
ENCARGADOS DE TRATAMIENTO

<Cuando el acceso de un tercero a los datos del responsable del fichero sea necesario para la prestación de un servicio a este último, no se considera que exista comunicación de datos. Recoger aquí el contrato que deberá constar por escrito o de alguna otra forma que permita acreditar su celebración y contenido, y que establecerá expresamente que el encargado de tratamiento tratará los datos conforme a las instrucciones del responsable del tra-

tamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, y que no los comunicarán, ni siquiera para su conservación a otras personas.

El contrato estipulará las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento esta obligado a implementar>.

ANEXO VIII
REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

<Si el registro de entrada y salida de soportes al que se refiere el apartado de "Gestión de soportes y Documentos", y que es obligatorio a partir del nivel medio, se gestiona de forma no automatizada, recoger en este anexo la información al efecto, según lo indicado el artículo 97 del RLOPD>.

ANEXO IX
MEDIDAS ALTERNATIVAS

<En el caso de que no sea posible adoptar las medidas exigidas por el RLOPD en relación con la identificación de los soportes, los dispositivos de almacenamiento de los documentos o los sistemas de almacenamiento de la información, indicar las causas que justifican que ello no sea posible y las medias alternativas que se han adoptado>.

COMPROBACIONES PARA LA REALIZACIÓN DE LA AUDITORÍA DE SEGURIDAD

OBJETIVO

Determinar si se han establecido, si son adecuadas y si se cumplen las medidas de seguridad recogidas en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Su realización es obligatoria para ficheros de nivel medio y alto. Puede ser interna o externa. 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.

DETERMINACIÓN DEL ALCANCE DE LA AUDITORÍA

Se debe establecer cuáles son los ficheros con datos de carácter personal objeto de la auditoría, tratamientos sobre los mismos, sistemas de tratamiento, procedimientos, etc.

PLANIFICACIÓN

Determinar los recursos necesarios para llevar a cabo la auditoría, las fuentes de información, la ubicación del fichero o las instalaciones, etc.

RECOLECCIÓN DE DATOS

- Relación de ficheros, estructura y contenido.
- Políticas de seguridad y procedimientos (registro de incidencias, copias de respaldo y recuperación, Identificación y autorización, borrado de soportes, cifrado, etc.).
- Documento de Seguridad y auditorías anteriores (si las hubiese).
- Diseño físico y lógico de los sistemas de información.
- Relación de usuarios, accesos autorizados y sus funciones.
- Inventario de soportes y registro de entrada y salida de soportes.
- Registros de acceso e informes de revisión de los mismos.
- Entrevistas a usuarios, técnicos de sistemas, responsables, etc.
- Inspección visual.
- etc.

EVALUACIÓN DE LAS PRUEBAS

Se relacionan a continuación algunas comprobaciones que se pueden realizar para verificar el cumplimiento de las disposiciones del Reglamento:

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
ASPECTOS GENERALES		
TODOS	¿La clasificación del nivel de seguridad es adecuada respecto a la naturaleza de la información contenida en cada uno de los ficheros y su finalidad?	BÁSICO
	¿Se han creado, modificado o suprimido ficheros con datos de carácter personal desde la última auditoría?	
ENCARGADO DE TRATAMIENTO		
TODOS	¿Se realiza el tratamiento por persona distinta al responsable del fichero?, ¿se ha formalizado mediante contrato conforme lo establecido el artículo 12 de la LOPD?	BÁSICO
	Si la realización de este encargo se realiza en los locales del responsable ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?, ¿consta por escrito en el contrato el compromiso del personal del encargado de tratamiento respecto al cumplimiento de las medidas de seguridad recogidas en el Documento de Seguridad del responsable?	
	Cuando el tratamiento se realiza mediante acceso remoto a los sistemas del responsable ¿se le ha prohibido al encargado de tratamiento la incorporación de los datos a sistemas o soportes distintos de los del responsable?, ¿se ha hecho constar tal circunstancia en el Documento de Seguridad del responsable?	
	Si la prestación se hace en locales propios del encargado de tratamiento (distintos de los del responsable) ¿ha elaborado el encargado el documento de seguridad?, ¿identifica el fichero o tratamiento y el responsable del mismo?, ¿detalla las medidas de seguridad a implementar en relación con su tratamiento?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
PRESTACIÓN DE SERVICIO SIN ACCESO A DATOS PERSONALES		
TODOS	Si el tratamiento no afecta a datos personales ¿se han adoptado las medidas necesarias para limitar el acceso del personal a los datos personales, soportes y recursos?	BÁSICO
	Si se trata de personal ajeno ¿recoge el contrato la prohibición expresa de acceder a los datos personales, así como la obligación de secreto respecto a los datos que hubieran podido conocer con motivo de la prestación de servicio?	
DELEGACIÓN DE AUTORIZACIONES		
TODOS	¿Se han delegado las autorizaciones que el Reglamento atribuye al responsable en otras personas?, ¿se ha hecho constar en el Documento de Seguridad las personas habilitadas para otorgar estas autorizaciones y las personas en quienes recae dicha delegación?	BÁSICO
RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO		
TODOS	El almacenamiento de datos personales en dispositivos portátiles o los tratamientos fuera de los locales del responsable o del encargado ¿han sido autorizados expresamente por el responsable del fichero?, ¿consta dicha autorización en el Documento de Seguridad?	BÁSICO
	¿Se garantiza el nivel de seguridad correspondiente al tipo de fichero tratado?	
FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS		
TODOS	¿Cumplen el nivel de seguridad correspondiente?	BÁSICO
	¿Se han destruido o borrado cuando ya no han sido necesarios para los fines que motivaron su creación?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	DOCUMENTO DE SEGURIDAD	
TODOS	¿Ha elaborado el responsable del fichero el Documento de Seguridad?	BÁSICO
	¿Contiene los aspectos mínimos exigidos por el Reglamento?	
	¿Está el documento actualizado?, ¿se ha revisado cuando se han producido cambios relevantes desde la auditoría anterior?	
	¿Está su contenido adecuado a la normativa vigente en este momento en materia de seguridad de los datos de carácter personal?	
	¿Se ha indicado con qué periodicidad se deben cambiar las contraseñas?, ¿es inferior o igual a un año?	
	¿Se especifica cuál es el personal autorizado para la concesión, alteración o anulación de accesos autorizados sobre datos o recursos?	
	¿Se especifica cuál es el personal autorizado para acceder a los lugares donde se almacenan los soportes informáticos?	
	Si el tratamiento se realiza por cuenta de terceros ¿se han reflejado los ficheros afectados por el encargo, con referencia expresa al contrato, así como la identificación del responsable y el periodo de vigencia?	
	¿Se ha reflejado en el Documento de Seguridad si los datos personales se incorporan y tratan exclusivamente en los sistemas del encargado?	
	¿Se ha delegado en el encargado del tratamiento la llevanza del Documento de Seguridad para los ficheros objeto del contrato?, ¿se ha reflejado esta circunstancia en el contrato?	
	¿Establece la identidad del responsable o responsables de seguridad?, ¿se especifica si la designación es única para todos los ficheros o está diferenciada según el sistema de tratamiento utilizado?	MEDIO
	¿Contiene los procedimientos y controles periódicos a realizar para verificar el cumplimento de lo dispuesto en el propio documento?	
	¿Especifica qué medidas hay que adoptar en caso de desechado o reutilización de soportes?	
	¿Relaciona las personas que están autorizadas a acceder físicamente a los locales donde se ubican los sistemas de información?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
FUNCIONES Y OBLIGACIONES DEL PERSONAL		
TODOS	Están las funciones y obligaciones del personal con acceso a datos de carácter personal y los sistemas de información claramente definidos?	BÁSICO
	¿Están documentadas y reflejadas en el documento de seguridad?	
	¿Se han definido las funciones de control o autorizaciones delegadas por el responsable del fichero?	
	¿Conoce el personal las medidas de seguridad que afectan al desarrollo de sus funciones?	
	¿Conoce las consecuencias de su incumplimiento?	
REGISTRO DE INCIDENCIAS		
TODOS	¿Existe un procedimiento de notificación y gestión de incidencias de seguridad?, ¿el procedimiento está bien diseñado y es eficaz? ¿Conoce todo el personal afectado dicho procedimiento?	BÁSICO
	¿Existe un registro de incidencias donde se reflejen todos los datos exigidos en el Reglamento?, ¿se han registrado todas las incidencias ocurridas?	
	¿Se revisa periódicamente el registro de incidencias para su análisis y adopción de medidas correctoras de las incidencias anotadas?	
AUTOMATIZADO	¿Se han anotado las ejecuciones de los procedimientos de recuperación de datos realizados?	
	¿Figuran en estas anotaciones los datos exigidos por el Reglamento?	MEDIO
	¿Existe la autorización por escrito del responsable del fichero?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	CONTROL DE ACCESO	
TODOS	¿Los accesos autorizados de los usuarios se corresponden exclusivamente a los datos y recursos que precisan para el desarrollo de sus funciones?	BÁSICO
	¿Existen mecanismos que impidan que los usuarios accedan a datos o recursos distintos de los autorizados?	
	¿Existe una relación de usuarios?, ¿especifica qué datos y recursos tiene autorizados para cada uno de ellos? ¿Está actualizada?	
	¿La concesión, alteración o anulación de accesos autorizados sobre datos y recursos la realiza exclusivamente el personal autorizado para ello en el Documento de Seguridad?	
	¿Ha establecido el responsable del fichero los criterios conforme a los cuales se otorga la autorización de los accesos a los datos y a los recursos?	
	El personal ajeno al responsable que tiene acceso a los datos y recursos de éste ¿se encuentra sometido a las mismas condiciones y obligaciones que el personal propio?	
AUTOMATIZADO	¿El acceso a los locales donde se encuentran ubicados los sistemas de información se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?	MEDIO
NO AUTOMATIZADO	¿Se encuentran los archivadores u otros elementos de almacenamiento en áreas de acceso restringido dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente?, ¿están cerradas estas áreas mientras no sea preciso el acceso a los documentos incluidos en el fichero?	ALTO
	Si los locales del responsable no permiten disponer de un área de acceso restringido ¿ha adoptado el responsable medidas alternativas?, ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?, ¿se ha motivado adecuadamente?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	GESTION DE SOPORTES Y DOCUMENTOS	
TODOS	¿Está identificado el tipo de información contenido en el soporte o documento?	BÁSICO
	¿Existe y se mantiene un inventario de soportes?	
	¿Se almacenan los soportes o documentos en lugares de acceso restringido?	
	¿Existen mecanismos por los que solamente puedan acceder las personas autorizadas en el Documento de Seguridad?, ¿funcionan adecuadamente estos mecanismos?	
	¿Se ha dejado constancia en el Documento de Seguridad, si fuera el caso, de la imposibilidad de cumplir con las obligaciones establecidas en el Reglamento sobre identificación, inventariado y acceso a los soportes dadas sus características físicas?	
	¿La salida de soportes y documentos fuera de los locales donde se ubica el fichero está siendo autorizada por el responsable del fichero o está debidamente autorizada en el Documento de Seguridad?	
	¿Se están tomando las medidas adecuadas en el traslado de documentación para evitar la sustracción, perdida o acceso indebido durante su transporte?	
	Cuando se desecha un soporte o documento conteniendo datos de carácter personal ¿se adoptan las medidas adecuadas para evitar el acceso a la información o su recuperación posterior cuando se procede a su destrucción o borrado?, ¿son adecuadas estas medidas?	
	¿Se dan de baja en el inventario estos soportes o documentos desechados?	
	Para los soportes con datos de carácter personal considerados especialmente sensibles por la organización ¿se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto?, ¿son adecuados y cumplen su finalidad?	
	¿Existe un registro de entrada de soportes o documentos?, ¿y un registro de salida?	MEDIO
	¿Contienen estos registros de entrada y salida de soportes toda la información exigida en el Reglamento?	
	¿Las personas encargadas de la recepción y la entrega de soportes están debidamente autorizadas?, ¿Consta en el Documento de Seguridad dicha autorización?	
	¿Se han anotado todas las entradas y salidas de soportes?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	GESTION DE SOPORTES Y DOCUMENTOS (CONT.)	
AUTOMATIZADO	¿Se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto? ¿son adecuados y cumplen su finalidad?	ALTO
	¿La distribución de soportes se realiza de forma cifrada, o por otro mecanismo que garantice que no sea inteligible o manipulable durante el transporte?	
	¿Se cifran los datos en los dispositivos portátiles cuando éstos salen de las instalaciones del responsable del fichero?	
	Si fuera imprescindible el tratamiento de datos en dispositivos portátiles que no permitan el cifrado de datos ¿se ha hecho constar motivadamente en el Documento de Seguridad?, ¿se han adoptado medidas para minimizar los riesgos derivados de este tratamiento en entornos desprotegidos?, ¿son adecuadas?	
NO AUTOMATIZADO	¿Se adoptan medidas que impidan el acceso o manipulación de la información en los casos de traslado físico de la documentación contenida en un fichero?, ¿son apropiadas estas medidas?	
	La generación de copias o reproducción de documentos ¿se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?	
	¿Se destruyen las copias o reproducciones desechadas de forma que no se pueda acceder a la información contenida en las mismas?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	IDENTIFICACIÓN Y AUTENTICACIÓN	
AUTOMATIZADO	¿Existe una relación de usuarios con acceso autorizado?, ¿se mantiene actualizada?	BÁSICO
	¿Existen procedimientos de identificación y autenticación para dicho acceso?, ¿garantiza la correcta identificación del usuario?	
	El mecanismo de acceso y verificación de autorización de los usuarios ¿les identifica de forma inequívoca y personalizada?	
	¿Existe un procedimiento de asignación, distribución y almacenamiento de contraseñas?, ¿garantiza su confidencialidad e integridad?	
	¿Se cambian las contraseñas con la periodicidad establecida en el documento de seguridad?	
	¿Se almacenan las contraseñas de forma ininteligible mientras están en vigor?	
	¿Se limita el intento reiterado de acceso no autorizado al sistema?, ¿se anotan estos intentos en el registro de incidencias?	MEDIO

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	COPIAS DE RESPALDO Y RECUPERACIÓN	
AUTOMATIZADO	¿El responsable del fichero ha definido los procedimientos de realización de copias de respaldo y recuperación de los datos?, ¿es adecuada esta definición?	BÁSICO
	¿Están reflejados estos procedimientos en el Documento de Seguridad?	
	¿Ha verificado el responsable del fichero la correcta aplicación de estos procedimientos?, ¿realiza esta verificación cada seis meses?	
	¿Garantizan los procedimientos establecidos la reconstrucción de los datos al estado en que se encontraban antes de producirse la pérdida o destrucción?	
	Si esta pérdida o destrucción afecta a ficheros parcialmente automatizados ¿se ha procedido a grabar manualmente los datos?, ¿queda constancia motivada de este hecho en el Documento de Seguridad?	
	¿Se realizan copias de respaldo al menos semanalmente? Si no es así ¿se debe a que no ha habido actualizaciones en ese periodo?	
	¿Las pruebas previas a la implantación o modificación de los sistemas de información se realizan con datos reales? En caso afirmativo, ¿se están aplicando las mismas medidas de seguridad que las que le corresponde por la naturaleza de los datos que contiene?, ¿se anota su realización en el Documento de Seguridad?, ¿se hacen copias de seguridad previas a la realización de pruebas con datos reales?	
	¿Se conserva una copia de respaldo y de los procedimientos de recuperación de datos en lugar diferente al de los equipos que los tratan?	ALTO
	¿Cumple este lugar las medidas de seguridad exigidas en el Reglamento?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
REGISTRO DE ACCESOS		
AUTOMATIZADO	¿Existe el registro de accesos? En caso negativo ¿concurren en el responsable alguna de las circunstancias que le eximen de este requisito? ¿se ha hecho constar en el Documento de Seguridad?	ALTO
	¿Se está recogiendo en este registro la información mínima exigida en el Reglamento?	
	¿Los mecanismos que permiten el registro de estos accesos están directamente bajo el control del responsable de seguridad?	
	¿Existe la posibilidad de desactivar estos mecanismos?	
	¿Se conservan los datos registrados por un período mínimo de dos años?	
	¿Revisa el responsable de seguridad periódicamente la información registrada?	
	¿Realiza el responsable de seguridad un informe, al menos mensualmente, con el resultado de las revisiones realizadas y los problemas detectados?	
NO AUTOMATIZADO	¿El acceso a la documentación se realiza exclusivamente por personal autorizado?	
	¿Existen mecanismos para identificar los accesos realizados cuando los documentos son utilizados por múltiples usuarios?	
	¿Se ha establecido un procedimiento para registrar el acceso de personas no incluidas en el caso anterior?, ¿es adecuado?	
ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES		
AUTOMATIZADO	¿Los accesos a datos mediante redes de comunicaciones garantizan un nivel de seguridad equivalente a los accesos en modo local?	BÁSICO
AUTOMATIZADO	¿La transmisión de datos a través de redes se realiza de forma cifrada (o por cualquier otro mecanismos que garantice que la información no sea inteligible ni manipulada por terceros)?, ¿este mecanismo de cifrado es eficaz?	ALTO

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	AUDITORÍA	
TODOS	¿Se realiza la actual auditoría en el plazo establecido desde la anterior?	MEDIO
	Si ha habido modificaciones sustanciales en el sistema de información ¿se ha realizado a continuación una auditoría para verificar la adaptación, adecuación y eficacia de las medidas de seguridad?	
	¿Los informes de las auditorías anteriores incluían los datos, hechos y observaciones en los que se basaban sus dictámenes?	
	¿Se han implementado las medidas correctoras propuestas por auditorías anteriores?, ¿han sido eficaces y han corregido las deficiencias encontradas?	
	CRITERIOS DE ARCHIVO	
TODOS	¿Existe legislación específica con criterios para el archivo de soportes o documentos?, ¿garantizan estos criterios la conservación de documentos, la localización y consulta de la información?, ¿posibilitan el ejercicio de los derechos de oposición, acceso, rectificación y cancelación?	BÁSICO
	En caso de no existir legislación específica ¿ha establecido el responsable del fichero los criterios y procedimientos de actuación para el archivo de documentos?, ¿es adecuado este procedimiento?	
	ALMACENAMIENTO DE LA INFORMACIÓN	
NO AUTOMATIZADO	¿Los dispositivos de almacenamiento de documentos disponen de mecanismos que obstaculicen su apertura? Si sus características físicas no permiten adoptar esta medida ¿ha adoptado el responsable medidas que impidan el acceso de personas no autorizadas?	BÁSICO
	CUSTODIA DE SOPORTES	
NO AUTOMATIZADO	¿Se custodia correctamente la documentación cuando ésta no se encuentra archivada en los dispositivos de almacenamiento por estar en revisión o tramitación?, ¿se impide en todo momento que sea accedida por persona no autorizada?	BÁSICO

ELABORACIÓN DEL INFORME

- Debe dictaminar sobre:
- Adecuación de las medidas y controles establecidas a lo dispuesto en el Título VIII del Reglamento.
- Identificación de deficiencias y propuesta de medidas correctoras o complementarias.
- Incluirá los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.
- Será analizado por el responsable de seguridad, y elevará sus conclusiones al responsable del fichero para que adopte las medidas adecuadas.
- Deberá quedar a disposición de la Agencia Española de Protección de Datos.

PREGUNTAS FRECUENTES

NIVELES DE SEGURIDAD

¿Cuándo se aplica el nivel básico de seguridad a datos de salud?

El artículo 81.6 del Reglamento de desarrollo de la LOPD señala que "podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos."

Por tanto dos son los factores que deben concurrir necesariamente para aplicar medidas de nivel básico en este caso: 1) la existencia de una ley que imponga un deber cuyo cumplimiento obligue a tratar ciertos datos de salud; y 2) que dichos datos respondan a unas características concretas.

En el primer caso, y a título de ejemplo, pueden citarse las obligaciones contempladas en la legislación sobre IRPF o Seguridad social, que en los ficheros de nóminas obligan a tratar datos como el porcentaje de discapacidad o la existencia de una incapacidad laboral.

En el segundo caso, se podrá aplicar el nivel básico, tratándose de datos de salud, únicamente, en los siguientes tipos de dato:

DISCAPACIDAD	porcentaje, indicador "SI/NO"
Incapacidad laboral, enfermedad común, accidente laboral, enfermedad profesional	"SI/NO" fecha
Aptitud para el desempeño (por razones de salud)	"Apto/no apto".
Maternidad	"SI/NO"

La regulación del artículo. 81.6 RDLOPD establece una excepción y por tanto debe ser interpretada restrictivamente. Por tanto, si no se trata de esta tipología de datos personales no podrá aplicarse. De ahí que en el caso de que se incluya referencia a un dato específico de salud, como por ejemplo, la enfermedad concreta relacionada con el motivo de la baja laboral o un código que la identifique, el nivel aplicable será el ALTO.

Además debe existir una ley que imponga la obligación de tratar el dato y por ello, si en un fichero se incluye voluntariamente un dato del tipo "porcentaje de discapacidad" sin que exista obligación legal el nivel aplicable al fichero será ALTO.

Por último, la presencia aislada de alguno de estos datos no prejuzga necesariamente el nivel de seguridad aplicable. Así por ejemplo, la presencia de un dato del tipo apto/no apto en un fichero dedicado a la prevención de riesgos que incluya el historial clínico-laboral del trabajador no permite aplicar el nivel básico ya que, habida cuenta del contenido de la citada historia clínica procederá aplicar el nivel de seguridad ALTO.

- **¿Cuándo podrá aplicarse el nivel básico de medidas de seguridad a un fichero que contenga datos especialmente protegidos como la afiliación sindical?**

El artículo 81.5.a) permite aplicar el nivel básico en caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual 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.

Existen dos ejemplos en los que se aprecia con claridad el criterio para aplicar esta excepción. En primer lugar, en el caso de que se tenga previsto tratar el dato relativo a las cuotas sindicales se deberá tener en cuenta que la deducción de la cuota sindical es una obligación impuesta por Ley al empresario. Así, el artículo 11 de la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical, establece que:

- *En los convenios colectivos podrán establecerse cláusulas por las que los trabajadores incluidos en su ámbito de aplicación atiendan económicamente la gestión de los sindicatos representados de la comisión negociadora, fijando un canon económico y regulando las modalidades de su abono. En todo caso, se respetará la voluntad individual del trabajador, que deberá expresarse por escrito en la forma y plazos que se determinen en la negociación colectiva.*

- *El empresario procederá al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de éste*".

Si atendemos al precepto anterior resulta claro que se impone al empresario un deber que se traduce en practicar un descuento y transferirlo al sindicato, es evidente que los datos relativos a la afiliación sindical son datos especialmente protegidos conforme al artículo 7 LOPD. No obstante, la excepción del Reglamento permite adoptar las medidas de seguridad de nivel básico.

Del mismo modo, y en segundo lugar, idéntica situación se produce en el caso de domiciliaciones bancarias para el pago de cuotas a sindicatos, partidos, confesiones, asociaciones etc. en los que la que el banco o caja trata los datos con la única finalidad de realizar la gestión consistente en un pago.

¿Qué se entiende por ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan datos especialmente protegidos?

En relación con el nivel de medidas de seguridad aplicable, sería necesario atender al tenor literal del artículo 81.5 del RLOPD que establece que "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 accesoria se contengan aquellos datos sin guardar relación con su finalidad."

A este respecto, se debería tener en cuenta que la excepción prevista en el último inciso del artículo 81.5 se refiere a cuando los datos especialmente protegidos sean incluidos por el propio afectado a la hora al presentar documentación en la que por propia iniciativa desee aportar este tipo de datos, sin que su tratamiento tenga relación con la finalidad establecida por el responsable del fichero.

Es fundamental tener en cuenta que esta excepción únicamente se aplicara a los ficheros no automatizados.

¿Qué nivel de seguridad debe adoptarse en los ficheros que contengan datos de menores?

En esta materia el RLOPDen su artículo 13, únicamente regula la forma de recabar el consentimiento de los menores, sin que ello afecte, en modo alguno, a las medidas de seguridad que deben de adaptarse a los ficheros o tratamientos de datos por parte del responsable.

La regulación de las medidas de seguridad, se encuentran en el Título VIII, Capítulo I artículos del 79 al 86. Así el artículo 80 señala que "Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto." Por otra parte el artículo 81 regula la aplicación estos niveles de seguridad.

Por lo tanto, la determinación del nivel de seguridad que debe de adoptar un responsable dependerá de los criterios fijados por el artículo 81 del Reglamento para el que la condición de la minoría de edad no es relevante.

ENCARGADOS Y PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS

¿Qué obligaciones en materia de medidas de seguridad tienen los encargados de tratamiento?

Tanto las prestaciones de servicios realizadas por los encargados de tratamiento en los locales del responsable del fichero, como las realizadas en los propios locales del encargado, se encuentran sujetas a la normativa de protección de datos.

Con carácter general, las obligaciones del encargado del tratamiento en materia de implantación de las medidas de seguridad se encuentran reguladas en los artículos 82 y 88 del Reglamento de desarrollo de la LOPD. Además el documento de seguridad de un encargado debe tener un contenido adicional específico que permita identificar sus encargos indicando:

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

En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a los restantes requisitos establecidos en el Reglamento de la LOPD.

Por último, el encargado de tratamiento debe implantar las medidas de seguridad adecuadas para sus propios ficheros. Entre ellas, debe mantener actualizado su documento de seguridad, fijar las obligaciones de su personal etc.

¿Puede el encargado hacerse cargo del documento de seguridad del responsable que le ha contratado?

No es infrecuente la existencia de tratamientos, como por ejemplo la confección de nóminas, en los que los datos se alojan y tratan casi por completo en los locales, recursos y soportes del encargado. Para estos casos, el reglamento se refiere en su artículo 88 a la "delegación de la llevanza del documento de seguridad". Para ello deben cumplirse ciertos requisitos:

- Que los datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado.
- Que esta circunstancia afecte a parte o a la totalidad de los ficheros o tratamientos del responsable.
- Que la delegación se indique de modo expreso en el contrato celebrado al amparo del artículo 12 LOPD, con especificación de los ficheros o tratamientos afectados.

No podrá delegarse en el encargado la llevanza del documento de seguridad en lo relativo a aquellos datos contenidos en recursos propios del responsable.

En las prestaciones sin acceso a datos ¿qué obligaciones de seguridad existen?

Se deberá tener en cuenta que la mayoría de las actividades que supongan un contacto directo o indirecto con el sistema de información y/o con su entorno físico o lógico puede ser susceptible de poner en riesgo la seguridad de los datos.

Así por ejemplo, el servicio de seguridad que custodia las llaves de las instalaciones debe ser advertido de las políticas de control de acceso físico a las instalaciones y de las eventuales restricciones de acceso que se hayan fijado.

Del mismo modo, los servicios de limpieza deberían ser informados de aspectos relacionados con las prohibiciones relacionadas con el desechado de documentos, -por ejemplo, utilizar medios convencionales como el contenedor de basuras-, o de la necesidad de que en determinadas salas se mantengan condiciones de refrigeración que garanticen la estabilidad de las máquinas que soportan el sistema de información.

Un último ejemplo, lo proporcionan los servicios de mantenimiento que, eventualmente, deben tener obligaciones cuando sus acciones pueden poner en peligro un sistema, - por ejemplo, la de advertir cuando una reparación haga necesario desconectar la red eléctrica obligando a un copiado y/o apagado preventivo.

En estos casos, para la realización de trabajos que no impliquen el tratamiento de datos personales, y de conformidad con lo establecido en el artículo 83 del Reglamento de la LOPD, el responsable del fichero debe adoptar las medidas adecuadas para limitar el acceso del personal a los datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios deberá recoger expresamente la prohibición de acceder a los datos personales y la obligación de secreto que el personal debe observar.

DOCUMENTO DE SEGURIDAD

□ ¿Qué debo hacer para documentar y/o notificar las funciones y obligaciones del personal?

La descripción de las funciones del personal con acceso a datos de carácter personal tienen que estar incluidas en el documento de seguridad y formarán parte de las medidas organizativas que el responsable del fichero y, en su caso, el encargado del tratamiento debe implantar.

El procedimiento de documentación y transmisión de las políticas que incluyan las funciones y obligaciones del personal con acceso a datos de carácter personal, puede ser diverso dependiendo de las particularidades de cada organización, pudiendo utilizarse documentos escritos, comunicaciones electrónicas, ya sea mediante correo electrónico, intranet corporativa, páginas de inicio de las aplicaciones, etc.

En todo caso, será necesario que el responsable del fichero y, en su caso, el encargado del tratamiento se aseguren que el personal con acceso a datos de carácter personal conoce las funciones y obligaciones que tiene con respecto al acceso a los datos de carácter personal, en particular, en lo relativo al deber de secreto y confidencialidad.

□ ¿Qué permite la delegación de autorizaciones?

La delegación de autorizaciones, a la que se refiere el artículo 84 del Reglamento, es una posibilidad que permite flexibilizar la gestión de la seguridad en materia de protección de datos de carácter personal.

Esta previsión habilita al responsable para delegar en otras personas las funciones que el Reglamento atribuye al responsable del fichero. Estas delegaciones deben estar recogidas en el documento de seguridad y no suponen, en ningún caso, trasladar a la persona en quien se delega la responsabilidad en la que pudiera incurrir la organización o persona responsable del fichero.

□ ¿Debe contener el registro de incidencias detalle de los problemas asociados a aspectos puramente técnicos de los ficheros: averías, caídas de tensión, problemas de red o conectividad?

El objetivo fundamental de implantar las medidas de seguridad a las que se refiere la LOPD (art. 9) y su Reglamento de desarrollo es garantizar que los datos de carácter personal se tratan con las adecuadas garantías que permitan asegurar la confidencialidad, la integridad y la disponibilidad de los datos.

En éste ámbito las incidencias poseen una gran relevancia debido tanto a su propia capacidad para comprometer los objetivos de la seguridad como por el conocimiento que su resolución aporta a los responsables. Así, por ejemplo una avería eléctrica puede poner en peligro la disponibilidad de un sistema de información.

Teniendo en cuenta los objetivos de la seguridad, la inclusión de las incidencias de este tipo deberá realizarse siempre cuando con motivo del funcionamiento de estos servicios la seguridad pudiera verse comprometida.

□ ¿Cuál es el alcance y el objetivo del registro de incidencias?

La obligación de establecer un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal, así como establecer un registro en el que se hagan constar los detalles de dichas incidencias, se encuentra regulado en el artículo 90 y 100 del Reglamento, dependiendo que el nivel de medidas de seguridad requeridas sea básico o medio.

El objetivo final perseguido por el Reglamento a este respecto, tal y como lo señala en el artículo 90 citado, es que se adopten las medidas correctoras para que dicha incidencia sea controlada, por lo que debe mantenerse una acción permanente de control, revisión y actuación sobre las medidas implantadas y las incidencias detectadas.

□ ¿Cuál es el alcance de la obligación de anotar las salidas de soportes mediante correo electrónico?

El envío de ficheros con datos de carácter personal mediante correo electrónico o fax conlleva ciertos riesgos específicos que deberán ser analizados por el responsable del fichero y, en su caso, por el encargado del tratamiento para establecer las medidas técnicas y organizativas que deben implantarse para controlar los riesgos inherentes a la utilización del dichos medios, en función de los tipos de datos que vayan ser objeto de transmisión.

En cualquier caso, tal y como establece el artículo 92 del Reglamento la salida de soportes y documentos que contengan datos de carácter personal, como los incluidos 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 o ser debidamente autorizada en el documento de seguridad.

En el caso de los ficheros que deben implantar las medidas catalogadas como de nivel medio, el artículo 97 del Reglamento establece la obligación de disponer de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer la información relacionada con el envío. En el caso de las medidas de seguridad de nivel alto, la distribución de los soportes deberá realizarse cifrando los datos o utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte (art. 101 Reglamento).

Por lo que respecta concretamente al sistema de registro, en el caso de que se remitan datos de carácter personal incluidos en un anexo a un correo electrónico, el propio gestor del correo electrónico puede servir como registro.

Esta obligación de anotar las salidas afecta a cualquier otro procedimiento electrónico como el protocolo FTP, descargas desde Internet, carpetas compartidas, así como al envío de fax cuando incorporan datos de carácter personal de un fichero o tratamiento.

- **¿Debe registrarse la salida de soportes con destino a otra sede de la entidad? ¿Y a la del encargado?**

Deben anotarse tanto en uno como en el otro caso, ya que se trata de asegurar el control y la trazabilidad de los soportes con datos de carácter personal que salen materialmente del sistema de información del responsable del fichero.

¿Debe notificarse a la AEPD el documento de seguridad?

El documento de seguridad es un documento interno de la organización y no debe ser notificado a la Agencia Española de Protección de Datos, quedando a disposición de la Agencia o, en su caso, de las autoridades de protección de datos de las Comunidades Autónomas.

MEDIDAS CONCRETAS

¿Qué significa guardar las copias de respaldo en lugar físico diferente?

Para los ficheros con datos de carácter personal sujetos a la obligación de implantar las medidas de nivel alto, el reglamento de desarrollo de la LOPD prevé la obligación de conservar una copia de respaldo de los datos de estos ficheros y de los procedimientos de recuperación de los mismos en un lugar diferente del que se encuentran los equipos informáticos que los tratan (art. 102 Reglamento LOPD), con el fin de que no se encuentren sometidos a las mismas contingencias que pudiera sufrir el lugar habitual de almacenamiento en caso de un accidente o desastre, como por ejemplo, un incendio o una inundación.

En el caso de que no sea posible guardar una copia de los ficheros en un lugar distinto y no sujeto a los mismos riesgos, se deberán adoptar medidas complementarias para paliar el riesgo, tales como ubicar la copia en armarios ignífugos, implantación de sistemas antiincendio, etc). En estos casos, cuando la sede del responsable cuente con distintas estancias o niveles de edificación se entenderá por lugar distinto una estancia diferenciada del lugar principal en el que se ubiquen los sistemas de información, preferiblemente en planta distinta y más protegida y, se deberá hacer constar estas circunstancias en el documento de seguridad.

Debe hacerse notar que la obligación de realizar copias de respaldo no es aplicable a los ficheros no automatizados, con independencia del resto de medidas aplicables e este tipo de ficheros, entre las que deberán observarse las previsiones establecidas en el Reglamento

de la LOPD, entre otras, en lo relativo a la custodia de los soportes y dispositivos de almacenamiento, así como a la copia o reproducción de los documentos con datos de carácter personal.

- **¿Cuál es el ámbito de la auditoría establecida en el RLOPD? ¿Quién debe realizarla? ¿Debe notificarse?**

El ámbito de la auditoría, previsto en el artículo 96 para los ficheros automatizados y 110 para los no automatizados, se refiere a la verificación del cumplimiento de las medidas de seguridad que deben implantarse en los ficheros automatizados y no automatizados con datos de carácter personal establecidas en el Título VIII del Reglamento de desarrollo de la LOPD, sin perjuicio de que cuando alguna de las materias reguladas la LOPD se proyecten sobre las medidas de seguridad deban ser tenidas en cuenta.

Así por ejemplo, es evidente que una salida de datos podría tener relación con una comunicación de datos pudiendo analizarse su licitud. Del mismo modo, la existencia de un encargado del tratamiento puede comportar una evaluación conexa del contenido del contrato.

Sobre quién debe realizarla, el Reglamento establece que puede ser interna o externa y no define el perfil funcional o profesional de los auditores, aunque la propia función de auditoría ha de llevar implícita la independencia y la debida capacitación profesional para que resulte adecuada para la función de verificación que pretende llevar a cabo.

Por último, el informe de auditoría deberá ser analizado por el responsable de seguridad que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de la comunidades autónomas, no siendo necesario su notificación a la AEPD.

¿Cuál debe ser el alcance del registro de accesos?

La obligación de implantar y guardar, durante un período mínimo de dos años, los datos relativos a los accesos realizados a los datos catalogados como de nivel alto, prevista en el artículo 103 del Reglamento de la LOPD, persigue que se pueda identificar el registro accedido. En este sentido, el objetivo es el de ser capaz de establecer las acciones realizadas por un determinado usuario respecto del registro accedido sin necesidad de que tal conocimiento alcance al contenido concreto de la información accedida.

El citado artículo establece la información mínima que deberá guardarse de cara acceso a los datos de carácter personal sujetos a la obligación de implantar las medidas de nivel alto.

Así mismo, se establecen las circunstancias concretas en las que el Reglamento excepciona de la obligación de implantar el registro de accesos: el responsable debe ser una persona física y debe ser el único usuario del sistema. Esta circunstancia deberá hacerse constar en el documento de seguridad.

¿Cómo aplico el control de acceso previsto para los ficheros no automatizados o manuales?

En el caso de los ficheros no automatizados con nivel alto de seguridad, el Reglamento de la LOPD establece, en su artículo 113 las medidas que han de adoptarse para controlar el acceso a la documentación a la que deba implantarse las medidas de nivel alto.

Para implantar este control de acceso a la documentación se podrán utilizar, por ejemplo:

- Plantillas básicas en soporte papel incorporadas al inicio del expediente.
- Registros automatizados en la gestión de entradas y salidas al archivo.
- Cualquier otro sistema o procedimiento que permita alcanzar la finalidad perseguida por el Reglamento.

OTROS ASPECTOS

En caso de una sanción por falta de medidas de seguridad ¿qué responsabilidad tiene el Responsable de Seguridad?

La responsabilidad de implantar las medidas de seguridad en los ficheros con datos de carácter personal recae en el responsable del fichero y, en su caso, en el encargado del tratamiento.

Así, entre las medidas organizativas se procederá a nombrar uno o varios responsables de seguridad. Esta designación es una previsión establecida en el Reglamento de la LOPD para los ficheros que tengan que implantar las medidas de seguridad catalogadas como de nivel medio y alto.

La medida que establece el artículo 95 del Reglamento, no puede suponer, en ningún caso, una exoneración de la responsabilidad que corresponda al responsable del fichero o al encargado del tratamiento.

- **¿Qué tengo que pedir al proveedor cuando adquiera un producto software que trate datos de carácter personal?**

La Disposición adicional única del Reglamento de desarrollo de la LOPD establece que los productos software destinados al tratamiento automatizado de datos de carácter personal deberán incluir en su descripción técnica el nivel de seguridad que tiene implantado, por lo que cuando se adquiera o se contrate la construcción de un aplicativo software que trate datos de carácter personal, se deberá pedir que el constructor especifique el nivel de medidas de seguridad que cumple el producto.

- **Para el cómputo de plazos para la implantación de las medidas de seguridad ¿cuándo se considera que son ficheros preexistentes?**

Se consideran ficheros preexistentes a los efectos de, en su caso, disponer del período transitorio para implantar las medidas de seguridad al que se refiere la Disposición transitoria segunda del Reglamento de desarrollo de la LOPD, los ficheros que hubieran sido notificados para su inscripción con anterioridad a la entrada en vigor del Reglamento de desarrollo de la LOPD, aprobado mediante el RD 1720/2007, de 21 de diciembre, publicado en el BOE del 19 de enero de 2008.

FICHEROS EXISTENTES		NIVEL	PLAZO
AUTOMATIZADOS	SEGURIDAD SOCIAL, MUTUAS, PERFILES	MEDIO	1 AÑO
	VIOLENCIA DE GÉNERO	MEDIO	1 AÑO
		ALTO	18 MESES
	TELECOMUNICACIONES (TRÁFICO, LOCALIZACIÓN) REGISTRO DE ACCESOS	MEDIO	1 AÑO 18 MESES
	ADAPTACIÓN RESTO DE FICHEROS		1 AÑO
NO AUTOMATIZADOS		BÁSICO	1 AÑO
		MEDIO	18 MESES
		ALTO	2 AÑOS

Dado que en la citada disposición se establecía la entrada en vigor del Reglamento a los tres meses de su publicación en el BOE, tendrán la consideración de ficheros preexistentes, a los efectos de la implantación de las medidas de seguridad, los ficheros que hayan sido notificados al Registro General de Protección de Datos hasta el día 19 de abril de 2008.

Cualquier fichero notificado con posterioridad deberá incorporar el conjunto de medidas previstas para el nivel de seguridad que le corresponda.

En la web de la Agencia Española de Protección de Datos, se encuentra disponible la versión actualizada de las preguntas frecuentes relacionadas con esta Guía de Seguridad.

www.agpd.es

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

www.agpd.es

Tríptico LSSI

La <Ley de Internet> fácil

Una Sociedad de la Información con mayores garantías

LSSI: Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES Y PARA LA SOCIEDAD DE LA INFORMACIÓN

Para las **empresas** que realizan **comercio electrónico**

La Ley se aplica al comercio electrónico y a otros servicios de Internet cuando sean parte de una actividad económica.

Obligaciones de información

- Deben mostrar en su página web, la siguiente información:
  - Su denominación social, NIF, domicilio y dirección de correo electrónico, teléfono o fax.
  - Los datos de inscripción registral.
  - Códigos de conducta a que estén adheridas.
  - Precios de los productos o servicios que ofrecen, con indicación de los impuestos y gastos de envío.
  - En su caso, datos relativos a la autorización administrativa necesaria para el ejercicio de la actividad; datos de colegiación y titulo académico de profesionales que ejerzan una actividad regulada; e información adicional cuando al servicio se acceda mediante un número de telefóno de tarificación adicional.

y si además realiza contratos on-line deberá añadir la siguiente información con carácter previo al proceso de contratación:

- Trámites que deben seguirse para contratar on-line.
- Si el documento electrónico del contrato se va a archivar y si éste será accesible.
- Medios técnicos para identificar y corregir errores en la introducción de datos.
- Lengua o lenguas en que podrá formalizarse el contrato.
- Condiciones generales a que, en su caso, se sujete el contrato.

...y confirmar la celebración del contrato por vía electrónica, mediante el envío de un acuse de recibo del pedido realizado.

...y si hacen **publicidad por vía electrónica**

Obligaciones

- El anunciante debe identificarse claramente.
- El carácter publicitario del mensaje debe resultar inequívoco.
- Si se realizan ofertas, concursos o juegos promocionales, además de lo anterior, se deberá:
  - Identificarlas como tales.
  - Expresar de forma clara e inequívoca las condiciones de participación.
- Cuando se envíen por correo electrónico, mensajes SMS...:
  - Obtener con carácter previo la solicitud o autorización expresa del destinatario.
  - Identificar el mensaje publicitario con la palabra « publicidad» o la abreviatura «publi».
  - Establecer procedimientos sencillos para facilitar revocación del consentimiento del usuario.

Para las **empresas** que prestan **servicios de intermediación** de la Sociedad de la información

Quiénes son

- Los operadores de telecomunicaciones; los proveedores de acceso a Internet (ISPs); los prestadores de servicios de alojamiento de datos, enlaces y buscadores.

Obligaciones

- Colaborar con los órganos públicos para la ejecución de resoluciones que no puedan cumplirse sin su ayuda.
- Informar a sus clientes sobre los diferentes medios técnicos que aumenten los niveles de seguridad de la información (anti-virus, anti-programas espía, filtros de correo); los aplicados por ellos; las herramientas existentes para el filtrado y restricción de acceso a determinados contenidos y servicios; y las posibles responsabilidades en que los usuarios pueden incurrir por eluso de internet con fines ilícitos. (ISPs).

Responsabilidad

- No son responsables de los contenidos que transmiten o alojan o a los que facilitan acceso, si no participan en su elaboración.
- Son responsables si conocen su ilicitud y no actúan rápidamente para retirarlos o imposibilitar el acceso a ellos.

Para los **usuarios** de **internet**

Titulares de páginas personales

- Solamente si incluyen publicidad por la que perciban ingresos están sujetas a la Ley. En ese caso, deben ofrecer información básica (nombre, residencia, dirección de correo electrónico, teléfono o fax y NIF) y respetar las normas de publicidad incluidas en la Ley:
  - El anunciante debe identificarse claramente.
  - El carácter publicitario de la información debe resultar inequívoco.

La LSSI ofrece nuevas garantías y derechos en Internet

- Derecho a obtener información sobre los prestadores de servicios (nombre, domicilio, dirección de correo electrónico, etc.) los precios de los productos o servicios que ofrecen, con indicación de los impuestos y gastos de envío.
- Respecto a la publicidad, derecho a conocer la identidad del anunciante, a no recibir mensajes promocionales no solicitados y a dejar de recibir los que hubiera autorizado.
- En la contratación, derecho a conocer los pasos necesarios para contratar por Internet, a acceder a las condiciones generales de la contratación antes de realizar su pedido y a obtener un acuse de recibo del vendedor que le asegure que su pedido ha llegado al vendedor.
- Si el consumidor realiza una compra a través de Internet, además se beneficia del régimen de protección que contempla la Ley de ordenación del comercio minorista para todas las ventas a distancia.

Información y consultas

En Internet

www.lssi.es

- Preguntas más frecuentes.
- Aspectos destacados de la Ley.
- Normativa en relación con los servicios de la sociedad de la información y el comercio electrónico.
- Enlaces con otras páginas de interés.

Por correo electrónico

Puedes enviar tus consultas a:

info@mityc.es

Por teléfono

Llamando al:

902 446 006

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
WWW.MITYC.ES

MINISTERIO DE SANIDAD Y CONSUMO
WWW.MSC.ES

MINISTERIO DE ECONOMÍA Y HACIENDA
WWW.MEH.ES

MINISTERIO DE JUSTICIA
WWW.JUSTICIA.ES

*Este folleto contiene información de carácter divulgativo, no exhaustivo

Edita: © SECRETARÍA DE ESTADO DE TELECOMUNICACIONES Y PARA LA SOCIEDAD DE LA INFORMACIÓN. Ministerio de la Sociedad de la Información

Ley Orgánica de Protección de Datos 15/1999

I. Disposiciones generales

JEFATURA DEL ESTADO

23750 *LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren. Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente Ley Orgánica tiene por objeto 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.

Artículo 2. *Ámbito de aplicación.*

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

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

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. *Definiciones.*

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II

Principios de la protección de datos

Artículo 4. *Calidad de los datos.*

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. *Derecho de información en la recogida de datos.*

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. 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 o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia 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.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. *Consentimiento del afectado.*

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. *Datos especialmente protegidos.*

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. *Datos relativos a la salud.*

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. *Seguridad de los datos.*

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. *Deber de secreto.*

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. *Comunicación de datos.*

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. *Acceso a los datos por cuenta de terceros.*

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

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

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III

Derechos de las personas

Artículo 13. *Impugnación de valoraciones.*

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. *Derecho de consulta al Registro General de Protección de Datos.*

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. *Derecho de acceso.*

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. *Derecho de rectificación y cancelación.*

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 17. *Procedimiento de oposición, acceso, rectificación o cancelación.*

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. *Tutela de los derechos.*

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los

interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. *Derecho a indemnización.*

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

Artículo 20. *Creación, modificación o supresión.*

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. *Comunicación de datos entre Administraciones públicas.*

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. *Ficheros de las Fuerzas y Cuerpos de Seguridad.*

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. *Excepciones a los derechos de acceso, rectificación y cancelación.*

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del

artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. *Otras excepciones a los derechos de los afectados.*

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. *Creación.*

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. *Notificación e inscripción registral.*

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. *Comunicación de la cesión de datos.*

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. *Datos incluidos en las fuentes de acceso público.*

1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.

Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.

En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. *Prestación de servicios de información sobre solvencia patrimonial y crédito.*

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos

de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. *Tratamientos con fines de publicidad y de prospección comercial.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. *Censo promocional.*

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.

3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. *Códigos tipo.*

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V

Movimiento internacional de datos

Artículo 33. *Norma general.*

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. *Excepciones.*

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.
k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

Agencia de Protección de Datos

Artículo 35. *Naturaleza y régimen jurídico.*

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.
2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.
3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.
4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.
b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. *El Director.*

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.
2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.
En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.
3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.
4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. *Funciones.*

Son funciones de la Agencia de Protección de Datos:

a) 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.
b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.
d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.
e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.
f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.
g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 38. *Consejo Consultivo.*

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por el Senado.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. *El Registro General de Protección de Datos.*

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones públicas.

b) Los ficheros de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. *Potestad de inspección.*

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. *Órganos correspondientes de las Comunidades Autónomas.*

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. *Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.*

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas

correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII

Infracciones y sanciones

Artículo 43. *Responsables.*

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. *Tipos de infracciones.*

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Artículo 45. *Tipo de sanciones.*

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. *Infracciones de las Administraciones públicas.*

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. *Prescripción.*

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. *Procedimiento sancionador.*

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

Artículo 49. *Potestad de inmovilización de ficheros.*

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Disposición adicional primera. *Ficheros preexistentes.*

Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Disposición adicional segunda. *Ficheros y Registro de Población de las Administraciones públicas.*

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.

Disposición adicional tercera. *Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.*

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos.

En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Disposición adicional cuarta. *Modificación del artículo 112.4 de la Ley General Tributaria.*

El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción:

«4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal.»

Disposición adicional quinta. *Competencias del Defensor del Pueblo y órganos autonómicos semejantes.*

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición adicional sexta. *Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.*

Se modifica el artículo 24.3, párrafo 2.º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción:

«Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado.»

Disposición transitoria primera. *Tratamientos creados por Convenios internacionales.*

La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Disposición transitoria segunda. *Utilización del censo promocional.*

Reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas. El Reglamento establecerá los plazos para la puesta en operación del censo promocional.

Disposición transitoria tercera. *Subsistencia de normas preexistentes.*

Hasta tanto se lleven a efectos las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

Disposición final primera. *Habilitación para el desarrollo reglamentario.*

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. *Preceptos con carácter de Ley ordinaria.*

Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria.

Disposición final tercera. *Entrada en vigor.*

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el «Boletín Oficial del Estado».

Por tanto,

Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta Ley Orgánica.

Madrid, 13 de diciembre de 1999.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ MARÍA AZNAR LÓPEZ

Ley de servicios de la sociedad de la información y de comercio electrónico 34/2002

I. Disposiciones generales

JEFATURA DEL ESTADO

13758 *LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.*

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren. Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

I

La presente Ley tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). Asimismo, incorpora parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de conformidad con lo establecido en ella, una acción de cesación contra las conductas que contravengan lo dispuesto en esta Ley.

Lo que la Directiva 2000/31/CE denomina «sociedad de la información» viene determinado por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información. Su incorporación a la vida económica y social ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo. Pero la implantación de Internet y las nuevas tecnologías tropieza con algunas incertidumbres jurídicas, que es preciso aclarar con el establecimiento de un marco jurídico adecuado, que genere en todos los actores intervinientes la confianza necesaria para el empleo de este nuevo medio.

Eso es lo que pretende esta Ley, que parte de la aplicación a las actividades realizadas por medios electrónicos de las normas tanto generales como especiales que las regulan, ocupándose tan sólo de aquellos aspectos que, ya sea por su novedad o por las peculiaridades que implica su ejercicio por vía electrónica, no están cubiertos por dicha regulación.

II

Se acoge, en la Ley, un concepto amplio de «servicios de la sociedad de la información», que engloba, además de la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.

Desde un punto de vista subjetivo, la Ley se aplica, con carácter general, a los prestadores de servicios establecidos en España. Por «establecimiento» se entiende el lugar desde el que se dirige y gestiona una actividad económica, definición esta que se inspira en el concepto de domicilio fiscal recogido en las normas tributarias españolas y que resulta compatible con la noción material de establecimiento predicada por el Derecho comunitario. La Ley resulta igualmente aplicable a quienes sin ser residentes en España prestan servicios de la sociedad de la información a través de un «establecimiento permanente» situado en España. En este último caso, la sujeción a la Ley es únicamente parcial, respecto a aquellos servicios que se presten desde España.

El lugar de establecimiento del prestador de servicios es un elemento esencial en la Ley, porque de él depende el ámbito de aplicación no sólo de esta Ley, sino de todas las demás disposiciones del ordenamiento español que les sean de aplicación, en función de la actividad que desarrollen. Asimismo, el lugar de establecimiento del prestador determina la ley y las autoridades competentes para el control de su cumplimiento, de acuerdo con el principio de la aplicación de la ley del país de origen que inspira la Directiva 2000/31/CE.

Por lo demás, sólo se permite restringir la libre prestación en España de servicios de la sociedad de la información procedentes de otros países pertenecientes al Espacio Económico Europeo en los supuestos previstos en la Directiva 2000/31/CE, que consisten en la producción de un daño o peligro graves contra ciertos valores fundamentales como el orden público, la salud pública o la protección de los menores. Igualmente, podrá

restringirse la prestación de servicios provenientes de dichos Estados cuando afecten a alguna de las materias excluidas del principio de país de origen, que la Ley concreta en su artículo 3, y se incumplan las disposiciones de la normativa española que, en su caso, resulte aplicable a las mismas.

III

Se prevé la anotación del nombre o nombres de dominio de Internet que correspondan al prestador de servicios en el registro público en que, en su caso, dicho prestador conste inscrito para la adquisición de personalidad jurídica o a los solos efectos de publicidad, con el fin de garantizar que la vinculación entre el prestador, su establecimiento físico y su «establecimiento» o localización en la red, que proporciona su dirección de Internet, sea fácilmente accesible para los ciudadanos y la Administración pública.

La Ley establece, asimismo, las obligaciones y responsabilidades de los prestadores de servicios que realicen actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en la red. En general, éstas imponen a dichos prestadores un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando. Las responsabilidades que pueden derivar del incumplimiento de estas normas no son sólo de orden administrativo, sino de tipo civil o penal, según los bienes jurídicos afectados y las normas que resulten aplicables.

Destaca, por otra parte, en la Ley, su afán por proteger los intereses de los destinatarios de servicios, de forma que éstos puedan gozar de garantías suficientes a la hora de contratar un servicio o bien por Internet. Con esta finalidad, la Ley impone a los prestadores de servicios la obligación de facilitar el acceso a sus datos de identificación a cuantos visiten su sitio en Internet; la de informar a los destinatarios sobre los precios que apliquen a sus servicios y la de permitir a éstos visualizar, imprimir y archivar las condiciones generales a que se someta, en su caso, el contrato. Cuando la contratación se efectúe con consumidores, el prestador de servicios deberá, además, guiarles durante el proceso de contratación, indicándoles los pasos que han de dar y la forma de corregir posibles errores en la introducción de datos, y confirmar la aceptación realizada una vez recibida.

En lo que se refiere a las comunicaciones comerciales, la Ley establece que éstas deban identificarse como tales, y prohíbe su envío por correo electrónico u otras vías de comunicación electrónica equivalente, salvo que el destinatario haya prestado su consentimiento.

IV

Se favorece igualmente la celebración de contratos por vía electrónica, al afirmar la Ley, de acuerdo con el principio espiritualista que rige la perfección de los contratos en nuestro Derecho, la validez y eficacia del consentimiento prestado por vía electrónica, declarar que no es necesaria la admisión expresa de esta técnica para que el contrato surta efecto entre las partes, y asegurar la equivalencia entre los documentos en soporte papel y los documentos electrónicos a efectos del cumplimiento del requisito de «forma escrita» que figura en diversas leyes.

Se aprovecha la ocasión para fijar el momento y lugar de celebración de los contratos electrónicos, adoptando una solución única, también válida para otros tipos de contratos celebrados a distancia, que unifica el criterio dispar contenido hasta ahora en los Códigos Civil y de Comercio.

Las disposiciones contenidas en esta Ley sobre aspectos generales de la contratación electrónica, como las relativas a la validez y eficacia de los contratos electrónicos o al momento de prestación del consentimiento, serán de aplicación aun cuando ninguna de las partes tenga la condición de prestador o destinatario de servicios de la sociedad de la información.

La Ley promueve la elaboración de códigos de conducta sobre las materias reguladas en esta Ley, al considerar que son un instrumento de autorregulación especialmente apto para adaptar los diversos preceptos de la Ley a las características específicas de cada sector. Por su sencillez, rapidez y comodidad para los usuarios, se potencia igualmente el recurso al arbitraje y a los procedimientos alternativos de resolución de conflictos que puedan crearse mediante códigos de conducta, para dirimir las disputas que puedan surgir en la contratación electrónica y en el uso de los demás servicios de la sociedad de la información. Se favorece, además, el uso de medios electrónicos en la tramitación de dichos procedimientos, respetando, en su caso, las normas que, sobre la utilización de dichos medios, establezca la normativa específica sobre arbitraje.

De conformidad con lo dispuesto en las Directivas 2000/31/CE y 98/27/CE, se regula la acción de cesación que podrá ejercitarse para hacer cesar la realización de conductas contrarias a la presente Ley que vulneren los intereses de los consumidores y usuarios. Para el ejercicio de esta acción, deberá tenerse en cuenta, además de lo dispuesto en esta Ley, lo establecido en la Ley general de incorporación de la Directiva 98/27/CE.

La Ley prevé, asimismo, la posibilidad de que los ciudadanos y entidades se dirijan a diferentes Ministerios y órganos administrativos para obtener información práctica sobre distintos aspectos relacionados con las materias objeto de esta Ley, lo que requerirá el establecimiento de mecanismos que aseguren la máxima coordinación entre ellos y la homogeneidad y coherencia de la información suministrada a los usuarios.

Finalmente, se establece un régimen sancionador proporcionado pero eficaz, como indica la Directiva 2000/31/CE, para disuadir a los prestadores de servicios del incumplimiento de lo dispuesto en esta Ley.

Asimismo, se contempla en la Ley una serie de previsiones orientadas a hacer efectiva la accesibilidad de las personas con discapacidad a la información proporcionada por medios electrónicos, y muy especialmente a la información suministrada por las Administraciones públicas, compromiso al que se refiere la resolución del Consejo de la Unión Europea de 25 de marzo de 2002, sobre accesibilidad de los sitios web públicos y de su contenido.

La presente disposición ha sido elaborada siguiendo un amplio proceso de consulta pública y ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio, y en el Real Decreto 1337/1999, de 31 de julio.

TÍTULO I

Disposiciones generales

CAPÍTULO I

Objeto

Artículo 1. *Objeto.*

1. Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en

lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

2. Las disposiciones contenidas en esta Ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia.

CAPÍTULO II

Ámbito de aplicación

Artículo 2. *Prestadores de servicios establecidos en España.*

1. Esta Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos.

Se entenderá que un prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

2. Asimismo, esta Ley será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad.

3. A los efectos previstos en este artículo, se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

La utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador.

4. Los prestadores de servicios de la sociedad de la información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización.

Artículo 3. *Prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo.*

1. Sin perjuicio de lo dispuesto en los artículos 7.1 y 8, esta Ley se aplicará a los prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a las materias siguientes:

a) Derechos de propiedad intelectual o industrial.

b) Emisión de publicidad por instituciones de inversión colectiva.

c) Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios.

d) Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.

e) Régimen de elección por las partes contratantes de la legislación aplicable a su contrato.

f) Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas.

2. En todo caso, la constitución, transmisión, modificación y extinción de derechos reales sobre bienes inmuebles sitos en España se sujetará a los requisitos formales de validez y eficacia establecidos en el ordenamiento jurídico español.

3. Los prestadores de servicios a los que se refiere el apartado 1 quedarán igualmente sometidos a las normas del ordenamiento jurídico español que regulen las materias señaladas en dicho apartado.

4. No será aplicable lo dispuesto en los apartados anteriores a los supuestos en que, de conformidad con las normas reguladoras de las materias enumeradas en el apartado 1, no fuera de aplicación la ley del país en que resida o esté establecido el destinatario del servicio.

Artículo 4. *Prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo.*

A los prestadores establecidos en países que no sean miembros de la Unión Europea o del Espacio Económico Europeo les será de aplicación lo dispuesto en los artículos 7.2 y 8.

Los prestadores que dirijan sus servicios específicamente al territorio español quedarán sujetos, además, a las obligaciones previstas en esta Ley, siempre que ello no contravenga lo establecido en tratados o convenios internacionales que sean aplicables.

Artículo 5. *Servicios excluidos del ámbito de aplicación de la Ley.*

1. Se regirán por su normativa específica las siguientes actividades y servicios de la sociedad de la información:

a) Los servicios prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas.

b) Los servicios prestados por abogados y procuradores en el ejercicio de sus funciones de representación y defensa en juicio.

2. Las disposiciones de la presente Ley, con la excepción de lo establecido en el artículo 7.1, serán aplicables a los servicios de la sociedad de la información relativos a juegos de azar que impliquen apuestas de valor económico, sin perjuicio de lo establecido en su legislación específica estatal o autonómica.

TÍTULO II

Prestación de servicios de la sociedad de la información

CAPÍTULO I

Principio de libre prestación de servicios

Artículo 6. *No sujeción a autorización previa.*

La prestación de servicios de la sociedad de la información no estará sujeta a autorización previa.

Esta norma no afectará a los regímenes de autorización previstos en el ordenamiento jurídico que no tengan por objeto específico y exclusivo la prestación por vía electrónica de los correspondientes servicios.

Artículo 7. *Principio de libre prestación de servicios.*

1. La prestación de servicios de la sociedad de la información que procedan de un prestador establecido en algún Estado miembro de la Unión Europea o del Espacio Económico Europeo se realizará en régimen de libre prestación de servicios, sin que pueda establecerse ningún tipo de restricciones a los mismos por razones derivadas del ámbito normativo coordinado, excepto en los supuestos previstos en los artículos 3 y 8.

2. La aplicación del principio de libre prestación de servicios de la sociedad de la información a prestadores establecidos en Estados no miembros del Espacio Económico Europeo se atendrá a los acuerdos internacionales que resulten de aplicación.

Artículo 8. *Restricciones a la prestación de servicios.*

1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

d) La protección de la juventud y de la infancia.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

2. Si para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un servicio o la retirada de datos procedentes de un prestador establecido en otro Estado, el órgano competente estimara necesario impedir el acceso desde España a los mismos, podrá ordenar a los prestadores de servicios de intermediación establecidos en España, directamente o mediante solicitud motivada al Ministerio de Ciencia y Tecnología, que tomen las medidas necesarias para impedir dicho acceso.

Será de aplicación lo dispuesto en el artículo 11 cuando los datos que deban retirarse o el servicio que deba interrumpirse procedan de un prestador establecido en España.

3. Las medidas de restricción a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda.

4. Fuera del ámbito de los procesos judiciales, cuando se establezcan restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, se seguirá el siguiente procedimiento:

a) El órgano competente requerirá al Estado miembro en que esté establecido el prestador afectado para que adopte las medidas oportunas. En el caso de que no las adopte o resulten insuficientes, dicho órgano notificará, con carácter previo, a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo y al Estado miembro de que se trate las medidas que tiene intención de adoptar.

b) En los supuestos de urgencia, el órgano competente podrá adoptar las medidas oportunas, notificándolas al Estado miembro de procedencia y a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo en el plazo de quince días desde su adopción. Asimismo, deberá indicar la causa de dicha urgencia.

Los requerimientos y notificaciones a que alude este apartado se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas.

CAPÍTULO II

Obligaciones y régimen de responsabilidad de los prestadores de servicios de la sociedad de la información

Sección 1.ª Obligaciones

Artículo 9. *Constancia registral del nombre de dominio.*

1. Los prestadores de servicios de la sociedad de la información establecidos en España deberán comunicar al Registro Mercantil en el que se encuentren inscritos, o a aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad, al menos, un nombre de dominio o dirección de Internet que, en su caso, utilicen para su identificación en Internet, así como todo acto de sustitución o cancelación de los mismos, salvo que dicha información conste ya en el correspondiente registro.

2. Los nombres de dominio y su sustitución o cancelación se harán constar en cada registro, de conformidad con sus normas reguladoras.

Las anotaciones practicadas en los Registros Mercantiles se comunicarán inmediatamente al Registro Mercantil Central para su inclusión entre los datos que son objeto de publicidad informativa por dicho Registro.

3. La obligación de comunicación a que se refiere el apartado 1 deberá cumplirse en el plazo de un mes desde la obtención, sustitución o cancelación del correspondiente nombre de dominio o dirección de Internet.

Artículo 10. *Información general.*

1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

a) Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

b) Los datos de su inscripción en el Registro a que se refiere el artículo 9.

c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

d) Si ejerce una profesión regulada deberá indicar:

1.º Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

2.º El título académico oficial o profesional con el que cuente.

3.º El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

4.º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.

f) Información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.

Artículo 11. *Deber de colaboración de los prestadores de servicios de intermediación.*

1. Cuando un órgano competente por razón de la materia hubiera ordenado, en ejercicio de las funciones que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, podrá ordenar a dichos prestadores, directamente o mediante solicitud motivada al Ministerio de Ciencia y Tecnología, que suspendan la transmisión, el alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de cualquier otro servicio equivalente de intermediación que realizaran.

2. En la adopción y cumplimiento de las medidas a que se refiere el apartado anterior, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

3. Las medidas a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda.

Artículo 12. *Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas.*

1. Los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo.

2. Los datos que, en cumplimiento de lo dispuesto en el apartado anterior, deberán conservar los operadores de redes y servicios de comunicaciones electrónicas y los proveedores de acceso a redes de telecomunicaciones serán únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información.

Los prestadores de servicios de alojamiento de datos deberán retener sólo aquéllos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio.

En ningún caso, la obligación de retención de datos afectará al secreto de las comunicaciones.

Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios a que se refiere este artículo no podrán utilizar los datos retenidos para fines distintos de los indicados en el apartado siguiente u otros que estén permitidos por la Ley, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos.

3. Los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales.

4. Reglamentariamente, se determinarán las categorías de datos que deberán conservarse según el tipo de servicio prestado, el plazo durante el que deberán retenerse en cada supuesto dentro del máximo previsto en este artículo, las condiciones en que deberán almacenarse, tratarse y custodiarse y la forma en que, en

su caso, deberán entregarse a los órganos autorizados para su solicitud y destruirse, transcurrido el plazo de retención que proceda, salvo que fueran necesarios para estos u otros fines previstos en la Ley.

SECCIÓN 2.ª RÉGIMEN DE RESPONSABILIDAD

Artículo 13. *Responsabilidad de los prestadores de los servicios de la sociedad de la información.*

1. Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley.

2. Para determinar la responsabilidad de los prestadores de servicios por el ejercicio de actividades de intermediación, se estará a lo establecido en los artículos siguientes.

Artículo 14. *Responsabilidad de los operadores de redes y proveedores de acceso.*

1. Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a ésta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos.

No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión.

2. Las actividades de transmisión y provisión de acceso a que se refiere el apartado anterior incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello.

Artículo 15. *Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios.*

Los prestadores de un servicio de intermediación que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, no serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos, si:

a) No modifican la información.

b) Permiten el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.

c) Respetan las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información.

d) No interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información, y

e) Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto tengan conocimiento efectivo de:

1.º Que ha sido retirada del lugar de la red en que se encontraba inicialmente.

2.º Que se ha imposibilitado el acceso a ella, o

3.º Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

Artículo 16. *Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos.*

1. Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador.

Artículo 17. *Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.*

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

CAPÍTULO III

Códigos de conducta

Artículo 18. *Códigos de conducta.*

1. Las Administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La Administración General del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional.

Los códigos de conducta podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información.

2. En la elaboración de dichos códigos, habrá de garantizarse la participación de las asociaciones de consumidores y usuarios y la de las organizaciones representativas de personas con discapacidades físicas o psíquicas, cuando afecten a sus respectivos intereses.

Cuando su contenido pueda afectarles, los códigos de conducta tendrán especialmente en cuenta la protección de los menores y de la dignidad humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias.

Los poderes públicos estimularán, en particular, el establecimiento de criterios comunes acordados por la industria para la clasificación y etiquetado de contenidos y la adhesión de los prestadores a los mismos.

3. Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales en la Comunidad Europea, con objeto de darles mayor difusión.

TÍTULO III

Comunicaciones comerciales por vía electrónica

Artículo 19. *Régimen jurídico.*

1. Las comunicaciones comerciales y las ofertas promocionales se regirán, además de por la presente Ley, por su normativa propia y la vigente en materia comercial y de publicidad.

2. En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales.

Artículo 20. *Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.*

1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y deberán indicar la persona física o jurídica en nombre de la cual se realizan.

En el caso en el que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra «publicidad».

2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación se expresen de forma clara e inequívoca.

Artículo 21. *Prohibición de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.*

Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

Artículo 22. *Derechos de los destinatarios de comunicaciones comerciales.*

1. Si el destinatario de servicios debiera facilitar su dirección de correo electrónico durante el proceso de contratación o de suscripción a algún servicio y el prestador pretendiera utilizarla posteriormente para el envío de comunicaciones comerciales, deberá poner en conocimiento de su cliente esa intención y solicitar su consentimiento para la recepción de dichas comunicaciones, antes de finalizar el procedimiento de contratación.

2. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

TÍTULO IV

Contratación por vía electrónica

Artículo 23. *Validez y eficacia de los contratos celebrados por vía electrónica.*

1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez.

Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.

2. Para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

3. Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico.

4. No será de aplicación lo dispuesto en el presente Título a los contratos relativos al Derecho de familia y sucesiones.

Los contratos, negocios o actos jurídicos en los que la Ley determine para su validez o para la producción de determinados efectos la forma documental pública, o que requieran por Ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica.

Artículo 24. *Prueba de los contratos celebrados por vía electrónica.*

1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico y, en su caso, a lo establecido en la legislación sobre firma electrónica.
2. En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental.

Artículo 25. *Intervención de terceros de confianza.*

1. Las partes podrán pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar. La intervención de dichos terceros no podrá alterar ni sustituir las funciones que corresponde realizar a las personas facultadas con arreglo a Derecho para dar fe pública.
2. El tercero deberá archivar en soporte informático las declaraciones que hubieran tenido lugar por vía telemática entre las partes por el tiempo estipulado que, en ningún caso, será inferior a cinco años.

Artículo 26. *Ley aplicable.*

Para la determinación de la ley aplicable a los contratos electrónicos se estará a lo dispuesto en las normas de Derecho internacional privado del ordenamiento jurídico español, debiendo tomarse en consideración para su aplicación lo establecido en los artículos 2 y 3 de esta Ley.

Artículo 27. *Obligaciones previas al inicio del procedimiento de contratación.*

1. Además del cumplimiento de los requisitos en materia de información que se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación de informar al destinatario de manera clara, comprensible e inequívoca, y antes de iniciar el procedimiento de contratación, sobre los siguientes extremos:

a) Los distintos trámites que deben seguirse para celebrar el contrato.
b) Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.
c) Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, y
d) La lengua o lenguas en que podrá formalizarse el contrato.

2. El prestador no tendrá la obligación de facilitar la información señalada en el apartado anterior cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o
b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación.

3. Sin perjuicio de lo dispuesto en la legislación específica, las ofertas o propuestas de contratación realizadas por vía electrónica serán válidas durante el período que fije el oferente o, en su defecto, durante todo el tiempo que permanezcan accesibles a los destinatarios del servicio.
4. Con carácter previo al inicio del procedimiento de contratación, el prestador de servicios deberá poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario.

Artículo 28. *Información posterior a la celebración del contrato.*

1. El oferente está obligado a confirmar la recepción de la aceptación al que la hizo por alguno de los siguientes medios:

a) El envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación, o
b) La confirmación, por un medio equivalente al utilizado en el procedimiento de contratación, de la aceptación recibida, tan pronto como el aceptante haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario.

En los casos en que la obligación de confirmación corresponda a un destinatario de servicios, el prestador facilitará el cumplimiento de dicha obligación, poniendo a disposición del destinatario alguno de los medios indicados en este apartado. Esta obligación será exigible tanto si la confirmación debiera dirigirse al propio prestador o a otro destinatario.
2. Se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello.
En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener la referida constancia desde que aquél haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones.
3. No será necesario confirmar la recepción de la aceptación de una oferta cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o
b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación.

Artículo 29. *Lugar de celebración del contrato.*

Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual.
Los contratos electrónicos entre empresarios o profesionales, en defecto de pacto entre las partes, se presumirán celebrados en el lugar en que esté establecido el prestador de servicios.

TÍTULO V

Solución judicial y extrajudicial de conflictos

CAPÍTULO I

Acción de cesación

Artículo 30. *Acción de cesación.*

1. Contra las conductas contrarias a la presente Ley que lesionen intereses colectivos o difusos de los consumidores podrá interponerse acción de cesación.
2. La acción de cesación se dirige a obtener una sentencia que condene al demandado a cesar en la conducta contraria a la presente Ley y a prohibir su reiteración futura. Asimismo, la acción podrá ejercerse para prohibir la realización de una conducta cuando ésta haya finalizado al tiempo de ejercitar la acción, si existen indicios suficientes que hagan temer su reiteración de modo inminente.
3. La acción de cesación se ejercerá conforme a las prescripciones de la Ley de Enjuiciamiento Civil para esta clase de acciones.

Artículo 31. *Legitimación activa.*

Están legitimados para interponer la acción de cesación:

a) Las personas físicas o jurídicas titulares de un derecho o interés legítimo.
b) Los grupos de consumidores o usuarios afectados, en los casos y condiciones previstos en la Ley de Enjuiciamiento Civil.
c) Las asociaciones de consumidores y usuarios que reúnan los requisitos establecidos en la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios, o, en su caso, en la legislación autonómica en materia de defensa de los consumidores.
d) El Ministerio Fiscal.
e) El Instituto Nacional del Consumo y los órganos correspondientes de las Comunidades Autónomas y de las Corporaciones Locales competentes en materia de defensa de los consumidores.
f) Las entidades de otros Estados miembros de la Unión Europea constituidas para la protección de los intereses colectivos o difusos de los consumidores que estén habilitadas ante la Comisión Europea mediante su inclusión en la lista publicada a tal fin en el «Diario Oficial de las Comunidades Europeas».

Los Jueces y Tribunales aceptarán dicha lista como prueba de la capacidad de la entidad habilitada para ser parte, sin perjuicio de examinar si la finalidad de la misma y los intereses afectados legitiman el ejercicio de la acción.

CAPÍTULO II

Solución extrajudicial de conflictos

Artículo 32. *Solución extrajudicial de conflictos.*

1. El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos a los arbitrajes previstos en la legislación de arbitraje y de defensa de los consumidores y usuarios, y a los procedimientos de resolución extrajudicial de conflictos que se instauren por medio de códigos de conducta u otros instrumentos de autorregulación.
2. En los procedimientos de resolución extrajudicial de conflictos a que hace referencia el apartado anterior, podrá hacerse uso de medios electrónicos, en los términos que establezca su normativa específica.

TÍTULO VI

Información y control

Artículo 33. *Información a los destinatarios y prestadores de servicios.*

Los destinatarios y prestadores de servicios de la sociedad de la información podrán dirigirse a los Ministerios de Ciencia y Tecnología, de Justicia, de Economía y de Sanidad y Consumo, y a los órganos que determinen las respectivas Comunidades Autónomas y Entidades Locales, para:

a) Conseguir información general sobre sus derechos y obligaciones contractuales en el marco de la normativa aplicable a la contratación electrónica.
b) Informarse sobre los procedimientos de resolución judicial y extrajudicial de conflictos, y
c) Obtener los datos de las autoridades, asociaciones u organizaciones que puedan facilitarles información adicional o asistencia práctica.

La comunicación con dichos órganos podrá hacerse por medios electrónicos.

Artículo 34. *Comunicación de resoluciones relevantes.*

1. El Consejo General del Poder Judicial remitirá al Ministerio de Justicia, en la forma y con la periodicidad que se acuerde mediante Convenio entre ambos órganos, todas las resoluciones judiciales que contengan pronunciamientos relevantes sobre la validez y eficacia de los contratos celebrados por vía electrónica, sobre su utilización como prueba en juicio, o sobre los derechos, obligaciones y régimen de responsabilidad de los destinatarios y los prestadores de servicios de la sociedad de la información.
2. Los órganos arbitrales y los responsables de los demás procedimientos de resolución extrajudicial de conflictos a que se refiere el artículo 32.1 comunicarán al Ministerio de Justicia los laudos o decisiones que revistan importancia para la prestación de servicios de la sociedad de la información y el comercio electrónico de acuerdo con los criterios indicados en el apartado anterior.
3. En la comunicación de las resoluciones, laudos y decisiones a que se refiere este artículo, se tomarán las precauciones necesarias para salvaguardar el derecho a la intimidad y a la protección de los datos personales de las personas identificadas en ellos.
4. El Ministerio de Justicia remitirá a la Comisión Europea y facilitará el acceso de cualquier interesado a la información recibida de conformidad con este artículo.

Artículo 35. *Supervisión y control.*

1. El Ministerio de Ciencia y Tecnología controlará el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información.

No obstante, las referencias a los órganos competentes contenidas en los artículos 8, 10, 11, 15, 16, 17 y 38 se entenderán hechas a los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia.

2. El Ministerio de Ciencia y Tecnología podrá realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos al Ministerio de Ciencia y Tecnología que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

3. En todo caso, y no obstante lo dispuesto en el apartado anterior, cuando las conductas realizadas por los prestadores de servicios de la sociedad de la información estuvieran sujetas, por razón de la materia o del tipo de entidad de que se trate, a ámbitos competenciales, de tutela o de supervisión específicos, con independencia de que se lleven a cabo utilizando técnicas y medios telemáticos o electrónicos, los órganos a los que la legislación sectorial atribuya competencias de control, supervisión, inspección o tutela específica ejercerán las funciones que les correspondan.

Artículo 36. *Deber de colaboración.*

1. Los prestadores de servicios de la sociedad de la información tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología y a los demás órganos a que se refiere el artículo anterior toda la información y colaboración precisas para el ejercicio de sus funciones.

Igualmente, deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la actividad de control de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.5 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

2. Cuando, como consecuencia de una actuación inspectora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, estatales o autonómicas, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

TÍTULO VII

Infracciones y sanciones

Artículo 37. *Responsables.*

Los prestadores de servicios de la sociedad de la información están sujetos al régimen sancionador establecido en este Título cuando la presente Ley les sea de aplicación.

Artículo 38. *Infracciones.*

1. Las infracciones de los preceptos de esta Ley se calificarán como muy graves, graves y leves.

2. Son infracciones muy graves:

a) El incumplimiento de las órdenes dictadas en virtud del artículo 8 en aquellos supuestos en que hayan sido dictadas por un órgano administrativo.

b) El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11.

c) El incumplimiento de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12.

d) La utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él.

3. Son infracciones graves:

a) El incumplimiento de lo establecido en los párrafos a) y f) del artículo 10.1.

b) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a destinatarios que no hayan autorizado o solicitado expresamente su remisión, o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando éste no hubiera solicitado o autorizado su remisión.

c) No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 27.

d) El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.

e) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.

4. Son infracciones leves:

a) La falta de comunicación al registro público en que estén inscritos, de acuerdo con lo establecido en el artículo 9, del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios de la sociedad de la información.

b) No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo.

c) El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.

d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a los destinatarios que no hayan solicitado o autorizado expresamente su remisión, cuando no constituya infracción grave.

e) No facilitar la información a que se refiere el artículo 27.1, cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.

f) El incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

Artículo 39. *Sanciones.*

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 150.001 hasta 600.000 euros.

La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España, durante un plazo máximo de dos años.

b) Por la comisión de infracciones graves, multa de 30.001 hasta 150.000 euros.

c) Por la comisión de infracciones leves, multa de hasta 30.000 euros.

2. Las infracciones graves y muy graves podrán llevar aparejada la publicación, a costa del sancionado, de la resolución sancionadora en el «Boletín Oficial del Estado», o en el diario oficial de la Administración pública que, en su caso, hubiera impuesto la sanción; en dos periódicos cuyo ámbito de difusión coincida con el de actuación de la citada Administración pública o en la

página de inicio del sitio de Internet del prestador, una vez que aquélla tenga carácter firme.

Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, el número de usuarios o de contratos afectados, y la gravedad del ilícito.

3. Cuando las infracciones sancionables con arreglo a lo previsto en esta Ley hubieran sido cometidas por prestadores de servicios establecidos en Estados que no sean miembros de la Unión Europea o del Espacio Económico Europeo, el órgano que hubiera impuesto la correspondiente sanción podrá ordenar a los prestadores de servicios de intermediación que tomen las medidas necesarias para impedir el acceso desde España a los servicios ofrecidos por aquéllos por un período máximo de dos años en el caso de infracciones muy graves, un año en el de infracciones graves y seis meses en el de infracciones leves.

Artículo 40. *Graduación de la cuantía de las sanciones.*

La cuantía de las multas que se impongan se graduará atendiendo a los siguientes criterios:

a) La existencia de intencionalidad.

b) Plazo de tiempo durante el que se haya venido cometiendo la infracción.

c) La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por resolución firme.

d) La naturaleza y cuantía de los perjuicios causados.

e) Los beneficios obtenidos por la infracción.

f) Volumen de facturación a que afecte la infracción cometida.

Artículo 41. *Medidas de carácter provisional.*

1. En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional previstas en dichas normas que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.

En particular, podrán acordarse las siguientes:

a) Suspensión temporal de la actividad del prestador de servicios y, en su caso, cierre provisional de sus establecimientos.

b) Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

c) Advertir al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

2. En la adopción y cumplimiento de las medidas a que se refiere el apartado anterior, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

3. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

4. En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en el presente artículo podrán ser acordadas antes de la iniciación del expediente sancionador. Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los quince días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Artículo 42. *Multa coercitiva.*

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Artículo 43. *Competencia sancionadora.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología, y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo.

Artículo 44. *Concurrencia de infracciones y sanciones.*

1. No podrá ejercerse la potestad sancionadora a que se refiere la presente Ley cuando haya recaído sanción penal, en los casos en que se aprecie identidad de sujeto, hecho y fundamento.

No obstante, cuando se esté tramitando un proceso penal por los mismos hechos o por otros cuya separación de los sancionables con arreglo a esta Ley sea racionalmente imposible, el procedimiento quedará suspendido respecto de los mismos hasta que recaiga pronunciamiento firme de la autoridad judicial.

Reanudado el expediente, en su caso, la resolución que se dicte deberá respetar los hechos declarados probados en la resolución judicial.

2. La imposición de una sanción prevista en esta Ley no impedirá la tramitación y resolución de otro procedimiento sancionador por los órganos u organismos competentes en cada caso cuando la conducta infractora

se hubiera cometido utilizando técnicas y medios telemáticos o electrónicos y resulte tipificada en otra Ley, siempre que no haya identidad del bien jurídico protegido.

3. No procederá la imposición de sanciones según lo previsto en esta Ley cuando los hechos constitutivos de infracción lo sean también de otra tipificada en la normativa sectorial a la que esté sujeto el prestador del servicio y exista identidad del bien jurídico protegido.

Cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

Artículo 45. *Prescripción.*

Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses; las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

Disposición adicional primera. *Significado de los términos empleados por esta Ley.*

A los efectos de la presente Ley, los términos definidos en el anexo tendrán el significado que allí se les asigna.

Disposición adicional segunda. *Medicamentos y productos sanitarios.*

La prestación de servicios de la sociedad de la información relacionados con los medicamentos y los productos sanitarios se regirá por lo dispuesto en su legislación específica.

Disposición adicional tercera. *Sistema Arbitral de Consumo.*

El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo.

La Junta Arbitral Nacional de Consumo y aquellas otras de ámbito territorial inferior, autorizadas para ello por el Instituto Nacional del Consumo, podrán dirimir los conflictos planteados por los consumidores de acuerdo con lo dispuesto en el Real Decreto 636/1993, de 3 de mayo, que regula el Sistema Arbitral de Consumo, a través de medios telemáticos.

Disposición adicional cuarta. *Modificación de los Códigos Civil y de Comercio.*

Uno. Se modifica el artículo 1.262 del Código Civil, que queda redactado de la siguiente manera:

«El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato.

Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.

En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.»

Dos. Se modifica el artículo 54 del Código de Comercio, que queda redactado de la siguiente manera:

«Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.

En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.»

Disposición adicional quinta. *Accesibilidad para las personas con discapacidad y de edad avanzada a la información proporcionada por medios electrónicos.*

Uno. Las Administraciones públicas adoptarán las medidas necesarias para que la información disponible en sus respectivas páginas de Internet pueda ser accesible a personas con discapacidad y de edad avanzada, de acuerdo con los criterios de accesibilidad al contenido generalmente reconocidos, antes del 31 de diciembre de 2005.

Asimismo, podrán exigir que las páginas de Internet cuyo diseño o mantenimiento financien apliquen los criterios de accesibilidad antes mencionados.

Dos. Igualmente, se promoverá la adopción de normas de accesibilidad por los prestadores de servicios y los fabricantes de equipos y «software», para facilitar el acceso de las personas con discapacidad o de edad avanzada a los contenidos digitales.

Disposición adicional sexta. *Sistema de asignación de nombres de dominio bajo el «.es».*

Uno. Esta disposición regula, en cumplimiento de lo previsto en la disposición adicional decimosexta de la Ley 17/2001, de 7 de diciembre, de Marcas, los principios inspiradores del sistema de asignación de nombres de dominio bajo el código de país correspondiente a España «.es».

Dos. La entidad pública empresarial Red.es es la autoridad de asignación, a la que corresponde la gestión del registro de nombres de dominio de Internet bajo el «.es», de acuerdo con lo establecido en la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.

Tres. La asignación de nombres de dominio de Internet bajo el «.es» se realizará de conformidad con los criterios que se establecen en esta disposición, en el Plan Nacional de Nombres de Dominio de Internet, en las demás normas específicas que se dicten en su desarrollo por la autoridad de asignación y, en la medida en que sean compatibles con ellos, con las prácticas generalmente aplicadas y las recomendaciones emanadas de las entidades y organismos internacionales que desarrollan actividades relacionadas con la gestión del sistema de nombres de dominio de Internet.

Los criterios de asignación de nombres de dominio bajo el «.es» deberán garantizar un equilibrio adecuado entre la confianza y seguridad jurídica precisas para el desarrollo del comercio electrónico y de otros servicios y actividades por vía electrónica, y la flexibilidad y agilidad requeridas para posibilitar la satisfacción de la demanda de asignación de nombres de dominio bajo el «.es», contribuyendo, de esta manera, al desarrollo de la sociedad de la información en España.

Podrán crearse espacios diferenciados bajo el «.es», que faciliten la identificación de los contenidos que alberguen en función de su titular o del tipo de actividad que realicen. Entre otros, podrán crearse indicativos relacionados con la educación, el entretenimiento y el adecuado desarrollo moral de la infancia y juventud. Estos

nombres de dominio de tercer nivel se asignarán en los términos que se establezcan en el Plan Nacional de Nombres de Dominio de Internet.

Cuatro. Podrán solicitar la asignación de nombres de dominio bajo el «.es», en los términos que se prevean en el Plan Nacional de Nombres de Dominio de Internet, todas las personas o entidades, con o sin personalidad jurídica, que tengan intereses o mantengan vínculos con España, siempre que reúnan los demás requisitos exigibles para la obtención de un nombre de dominio.

Los nombres de dominio bajo el «.es» se asignarán al primer solicitante que tenga derecho a ello, sin que pueda otorgarse, con carácter general, un derecho preferente para la obtención o utilización de un nombre de dominio a los titulares de determinados derechos.

La asignación de un nombre de dominio confiere a su titular el derecho a su utilización, el cual estará condicionado al cumplimiento de los requisitos que en cada caso se establezcan, así como a su mantenimiento en el tiempo. La verificación por parte de la autoridad de asignación del incumplimiento de estos requisitos dará lugar a la cancelación del nombre de dominio, previa la tramitación del procedimiento que en cada caso se determine y que deberá garantizar la audiencia de los interesados.

Los beneficiarios de un nombre de dominio bajo el «.es» deberán respetar las reglas y condiciones técnicas que pueda establecer la autoridad de asignación para el adecuado funcionamiento del sistema de nombres de dominio bajo el «.es».

La responsabilidad del uso correcto de un nombre de dominio de acuerdo con las leyes, así como del respeto a los derechos de propiedad intelectual o industrial, corresponde a la persona u organización para la que se haya registrado dicho nombre de dominio, en los términos previstos en esta Ley. La autoridad de asignación procederá a la cancelación de aquellos nombres de dominio cuyos titulares infrinjan esos derechos o condiciones, siempre que así se ordene en la correspondiente resolución judicial, sin perjuicio de lo que se prevea en aplicación del apartado ocho de esta disposición adicional.

Cinco. En el Plan Nacional de Nombres de Dominio de Internet se establecerán mecanismos apropiados para prevenir el registro abusivo o especulativo de nombres de dominio, el aprovechamiento indebido de términos de significado genérico o topónimos y, en general, para prevenir los conflictos que se puedan derivar de la asignación de nombres de dominio.

Asimismo, el Plan incluirá las cautelas necesarias para minimizar el riesgo de error o confusión de los usuarios en cuanto a la titularidad de nombres de dominio.

A estos efectos, la entidad pública empresarial Red.es establecerá la necesaria coordinación con los registros públicos españoles. Sus titulares deberán facilitar el acceso y consulta a dichos registros públicos, que, en todo caso, tendrá carácter gratuito para la entidad.

Seis. La asignación de nombres de dominio se llevará a cabo por medios telemáticos que garanticen la agilidad y fiabilidad de los procedimientos de registro. La presentación de solicitudes y la práctica de notificaciones se realizarán por vía electrónica, salvo en los supuestos en que así esté previsto en los procedimientos de asignación y demás operaciones asociadas al registro de nombres de dominio.

Los agentes registradores, como intermediarios en los procedimientos relacionados con el registro de nombres de dominio, podrán prestar servicios auxiliares para la asignación y renovación de éstos, de acuerdo con los requisitos y condiciones que determine la autoridad de asignación, los cuales garantizarán, en todo caso, el respeto al principio de libre competencia entre dichos agentes.

Siete. El Plan Nacional de Nombres de Dominio de Internet se aprobará mediante Orden del Ministro de Ciencia y Tecnología, a propuesta de la entidad pública empresarial Red.es.

El Plan se completará con los procedimientos para la asignación y demás operaciones asociadas al registro de nombres de dominio y direcciones de Internet que establezca el Presidente de la entidad pública empresarial Red.es, de acuerdo con lo previsto en la disposición adicional decimoctava de la Ley 14/2000, de 29 de diciembre, de Medidas fiscales, administrativas y del orden social.

Ocho. En los términos que permitan las disposiciones aplicables, la autoridad de asignación podrá establecer un sistema de resolución extrajudicial de conflictos sobre la utilización de nombres de dominio, incluidos los relacionados con los derechos de propiedad industrial. Este sistema, que asegurará a las partes afectadas las garantías procesales adecuadas, se aplicará sin perjuicio de las eventuales acciones judiciales que las partes puedan ejercitar.

Nueve. Con la finalidad de impulsar el desarrollo de la Administración electrónica, la entidad pública empresarial Red.es podrá prestar el servicio de notificaciones administrativas telemáticas y acreditar de forma fehaciente la fecha y hora de su recepción.

Disposición transitoria única. *Anotación en los correspondientes registros públicos de los nombres de dominio otorgados antes de la entrada en vigor de esta Ley.*

Los prestadores de servicios que, a la entrada en vigor de esta Ley, ya vinieran utilizando uno o más nombres de dominio o direcciones de Internet deberán solicitar la anotación de, al menos, uno de ellos en el registro público en que figuraran inscritos a efectos constitutivos o de publicidad, en el plazo de un año desde la referida entrada en vigor.

Disposición final primera. *Modificación del artículo 37 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el párrafo a) del apartado 1 del artículo 37 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que queda redactada en los siguientes términos:

> «a) Que los ciudadanos puedan recibir conexión a la red telefónica pública fija y acceder a la prestación del servicio telefónico fijo disponible para el público. La conexión debe ofrecer al usuario la posibilidad de emitir y recibir llamadas nacionales e internacionales y permitir la transmisión de voz, fax y datos a velocidad suficiente para acceder de forma funcional a Internet.
>
> A estos efectos, se considerará que la velocidad suficiente a la que se refiere el párrafo anterior es la que se utiliza de manera generalizada para acceder a Internet por los abonados al servicio telefónico fijo disponible para el público con conexión a la red mediante pares de cobre y módem para banda vocal.»

Disposición final segunda. *Modificación de la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el apartado 10 de la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de

Telecomunicaciones, que quedará redactado como sigue:

«10. Tasa por asignación del recurso limitado de nombres de dominio y direcciones de Internet.

a) Hecho imponible.

El hecho imponible de la tasa por asignación de nombres de dominio y direcciones de Internet estará constituido por la realización por la entidad pública empresarial Red.es de las actividades necesarias para la asignación y renovación de nombres de dominio y direcciones de Internet bajo el código de país correspondiente a España (.es).

b) Sujetos pasivos.

Serán sujetos pasivos de la tasa los solicitantes de la asignación o renovación de los nombres y direcciones de Internet.

c) Cuantía.

La cuantía de la tasa será única por cada nombre o dirección cuya asignación o renovación se solicite. En ningún caso se procederá a la asignación o a la renovación del nombre o dirección sin que se haya efectuado previamente el pago de la tasa.

Sólo podrán modificarse mediante Ley el número e identidad de los elementos y criterios de cuantificación con base en los cuales se determinan las cuotas exigibles.

A los efectos previstos en el párrafo anterior, se consideran elementos y criterios de cuantificación del importe exigible por asignación anual inicial de los nombres de dominio o direcciones de Internet el número asignado, el coste de las actividades de comprobación y verificación de las solicitudes de asignación, así como el nivel en que se produzca la asignación y, en el caso de renovación anual en los años sucesivos, el coste del mantenimiento de la asignación y de las actividades de comprobación y de actualización de datos. Igualmente, se atenderá al número de nombres o direcciones de Internet asignados y a la actuación a través de agentes registradores para concretar la cuantía de la tasa.

El establecimiento y modificación de las cuantías resultantes de la aplicación de los elementos y criterios de cuantificación a que se refieren los párrafos anteriores podrá efectuarse mediante Orden ministerial.

No obstante lo dispuesto en los párrafos anteriores de este apartado, en los supuestos de carácter excepcional en que así esté previsto en el Plan Nacional de Nombres de Dominio de Internet y en los términos que en el mismo se fijen, con base en el especial valor de mercado del uso de determinados nombres y direcciones, la cuantía por asignación anual inicial podrá sustituirse por la que resulte de un procedimiento de licitación en el que se fijará un valor inicial de referencia estimado. Si el valor de adjudicación de la licitación resultase superior a dicho valor de referencia, aquél constituirá el importe de la tasa. En los supuestos en que se siga este procedimiento de licitación, el Ministerio de Ciencia y Tecnología requerirá, con carácter previo a su convocatoria, a la autoridad competente para el Registro de Nombres de Dominio para que suspenda el otorgamiento de los nombres y direcciones que considere afectados por su especial valor económico. A continuación, se procederá a aprobar el correspondiente pliego de bases que establecerá, tomando en consideración lo previsto en el Plan Nacional de Nombres de Dominio de Internet, los requisitos, condiciones y régimen aplicable a la licitación.

d) Devengo.

La tasa se devengará en la fecha en que se proceda, en los términos que se establezcan reglamentariamente, a la admisión de la solicitud de asignación o de renovación de los nombres o direcciones de Internet, que no se tramitará sin que se haya efectuado el pago correspondiente.

e) Exacción y gestión recaudatoria.

La exacción de la tasa se producirá a partir de la atribución de su gestión a la entidad pública empresarial Red.es y de la determinación del procedimiento para su liquidación y pago, mediante Orden ministerial.

Los modelos de declaración, plazos y formas de pago de la tasa se aprobarán mediante resolución de la entidad pública empresarial Red.es.

El importe de los ingresos obtenidos por esta tasa se destinará a financiar los gastos de la entidad pública empresarial Red.es por las actividades realizadas en el cumplimiento de las funciones asignadas a la misma en los párrafos a), b), c) y d) del apartado 4 de esta disposición, ingresándose, en su caso, el excedente en el Tesoro Público, de acuerdo con la proporción y cuantía que se determine mediante resolución conjunta de las Secretarías de Estado de Presupuestos y Gastos y de Telecomunicaciones y para la Sociedad de la Información, a propuesta de esta última.»

Disposición final tercera. *Adición de una nueva disposición transitoria a la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se añade a la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, una nueva disposición transitoria duodécima, con la siguiente redacción:

«Disposición transitoria duodécima. *Criterios para el desarrollo del plan de actualización tecnológica de la red de acceso de la red telefónica pública fija.*

En el plazo máximo de cinco meses a partir de la entrada en vigor de esta disposición, el operador designado para la prestación del servicio universal presentará al Ministerio de Ciencia y Tecnología, para su aprobación en el plazo de un mes, previo informe de la Comisión del Mercado de las Telecomunicaciones, un plan de actuación detallado para garantizar que las conexiones a la red telefónica pública fija posibiliten a sus abonados el acceso funcional a Internet y, en particular, a los conectados mediante Telefonía Rural de Acceso Celular (TRAC).

El desarrollo del plan estará sujeto a las siguientes condiciones:

a) Incluirá soluciones tecnológicas eficientes disponibles en el mercado para garantizar el derecho de los usuarios a disponer, previa solicitud a partir de la aprobación del plan, de la posibilidad de acceso funcional a Internet en el plazo máximo de sesenta días desde la fecha de dicha solicitud en las zonas con cobertura. Estas soluciones tecnológicas deberán prever su evolución a medio plazo hacia velocidades de banda ancha sin que ello conlleve necesariamente su sustitución.

b) La implantación en la red de acceso de las soluciones tecnológicas a las que se refiere el párrafo a) deberá alcanzar a los abonados al servicio telefónico fijo disponible al público que, en la fecha de aprobación del plan, no tienen la posibilidad

de acceso funcional a Internet, de acuerdo con el siguiente calendario:

1.º Al menos al 30 por 100 antes del 30 de junio de 2003.
2.º Al menos al 70 por 100 antes del 31 de diciembre de 2003.
3.º El 100 por 100 antes del 31 de diciembre de 2004.

En todo caso, esta implantación alcanzará, al menos, al 50 por 100 de los citados abonados en cada una de las Comunidades Autónomas antes del 31 de diciembre de 2003.

c) En el plan de actuación deberá priorizarse el despliegue al que se refiere el párrafo b) con arreglo al criterio de mayor densidad de abonados afectados.

d) A los efectos de lo dispuesto en los apartados anteriores y en caso de que sea necesario, el operador designado para la prestación del servicio universal podrá concluir con otros operadores titulares de concesiones de dominio público radioeléctrico, contratos de cesión de derechos de uso de las bandas de frecuencias necesarias para el cumplimiento de los objetivos establecidos en esta disposición. Dichos contratos deberán ser sometidos a la previa aprobación por parte del Ministerio de Ciencia y Tecnología, que podrá establecer las condiciones de salvaguarda del interés público que estime necesarias.»

Disposición final cuarta. *Modificación de la disposición derogatoria única de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el último párrafo de la disposición derogatoria única de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que queda redactado de la siguiente forma:

«Igualmente, quedan derogadas cuantas otras disposiciones de igual o inferior rango a la presente Ley se opongan a lo dispuesto en ella y, en especial, a lo dispuesto en el artículo 37.1.a), en lo relativo a la velocidad de transmisión de datos.»

Disposición final quinta. *Adecuación de la regulación reglamentaria sobre contratación telefónica o electrónica con condiciones generales a esta Ley.*

El Gobierno, en el plazo de un año, modificará el Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación, para adaptar su contenido a lo dispuesto en esta Ley.

En dicha modificación, el Gobierno tendrá especialmente en cuenta la necesidad de facilitar la utilización real de los contratos electrónicos, conforme al mandato recogido en el artículo 9.1 de la Directiva 2000/31/CE.

Disposición final sexta. *Fundamento constitucional.*

Esta Ley se dicta al amparo del artículo 149.1.6.ª, 8.ª y 21.ª de la Constitución, sin perjuicio de las competencias de las Comunidades Autónomas.

Disposición final séptima. *Habilitación al Gobierno.*

Se habilita al Gobierno para desarrollar mediante Reglamento lo previsto en esta Ley.

Disposición final octava. *Distintivo de adhesión a códigos de conducta que incorporen determinadas garantías.*

En el plazo de un año a partir de la entrada en vigor de esta Ley, el Gobierno aprobará un distintivo que permita identificar a los prestadores de servicios que respeten códigos de conducta adoptados con la participación del Consejo de Consumidores y Usuarios, y que incluyan, entre otros contenidos, la adhesión al Sistema Arbitral de Consumo o a otros sistemas de resolución extrajudicial de conflictos que respeten los principios establecidos en la normativa comunitaria sobre sistemas alternativos de resolución de conflictos con consumidores, en los términos que reglamentariamente se establezcan.

Disposición final novena. *Entrada en vigor.*

Esta Ley entrará en vigor a los tres meses de su publicación en el «Boletín Oficial del Estado».

No obstante, las disposiciones adicional sexta y finales primera, segunda, tercera y cuarta de esta Ley entrarán en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Por tanto,
Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta Ley.

Madrid, 11 de julio de 2002.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ MARÍA AZNAR LÓPEZ

ANEXO

Definiciones

A los efectos de esta Ley, se entenderá por:

a) «Servicios de la sociedad de la información» o «servicios»: todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

1.º La contratación de bienes o servicios por vía electrónica.
2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
3.º La gestión de compras en la red por grupos de personas.
4.º El envío de comunicaciones comerciales.
5.º El suministro de información por vía telemática.
6.º El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las caracte-

rísticas señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

1.º Los servicios prestados por medio de telefonía vocal, fax o télex.

2.º El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

3.º Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

4.º Los servicios de radiodifusión sonora, y

5.º El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

b) «Servicio de intermediación»: servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información.

Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.

c) «Prestador de servicios» o «prestador»: persona física o jurídica que proporciona un servicio de la sociedad de la información.

d) «Destinatario del servicio» o «destinatario»: persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información.

e) «Consumidor»: persona física o jurídica en los términos establecidos en el artículo 1 de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

f) «Comunicación comercial»: toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica.

g) «Profesión regulada»: toda actividad profesional que requiera para su ejercicio la obtención de un título, en virtud de disposiciones legales o reglamentarias.

h) «Contrato celebrado por vía electrónica» o «contrato electrónico»: todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones.

i) «Ámbito normativo coordinado»: todos los requisitos aplicables a los prestadores de servicios de la sociedad de la información, ya vengan exigidos por la presente Ley u otras normas que regulen el ejercicio de actividades económicas por vía electrónica, o por las leyes generales que les sean de aplicación, y que se refieran a los siguientes aspectos:

1.º Comienzo de la actividad, como las titulaciones profesionales o cualificaciones requeridas, la publicidad registral, las autorizaciones administrativas o colegiales precisas, los regímenes de notificación a cualquier órgano u organismo público o privado, y

2.º Posterior ejercicio de dicha actividad, como los requisitos referentes a la actuación del prestador de servicios, a la calidad, seguridad y contenido del servicio, o los que afectan a la publicidad y a la contratación por vía electrónica y a la responsabilidad del prestador de servicios.

No quedan incluidos en este ámbito las condiciones relativas a las mercancías y bienes tangibles, a su entrega ni a los servicios no prestados por medios electrónicos.

j) «Órgano competente»: todo órgano jurisdiccional o administrativo, ya sea de la Administración General del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas.

MINISTERIO DE ECONOMÍA

13759 *ORDEN ECO/1758/2002, de 9 de julio, por la que se establecen los criterios generales de tramitación telemática de determinados procedimientos en materia de personal.*

El artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, prevé el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos por las Administraciones públicas en el desarrollo de su actividad y el ejercicio de sus funciones.

Tal previsión ha sido desarrollada por los Reales Decretos 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, y 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y la devolución de originales y el régimen y funcionamiento de las oficinas de Registro.

En este contexto, la iniciativa del Gobierno INFO XXI, aprobada en el Consejo de Ministros del día 23 de diciembre de 1999, ha supuesto un decidido impulso al desarrollo de la sociedad de la información al promover el uso de las nuevas tecnologías por las Administraciones públicas tanto en sus relaciones internas como en su vertiente externa de relación con los ciudadanos.

Prueba del interés por dotar a las Administraciones públicas de un nuevo instrumento de relación con los ciudadanos, es la modificación operada en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, por la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, en lo referente a la creación de registros telemáticos y a las notificaciones efectuadas por esa misma vía.

Finalmente, como corolario de todo lo anterior, el Ministerio de Economía ha desarrollado, por Orden de 26 de noviembre de 2001, los criterios generales de tramitación telemática de determinados procedimientos del Departamento y organismos públicos adscritos, así como también ha creado un Registro Telemático para la presentación de escritos y solicitudes.