BORRADOR DE REGLAMENTO DE DESARROLLO DE LA LOPD

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1 Objeto

El presente Reglamento tiene por objeto el desarrollo de los principios, derechos, obligaciones y procedimientos que garantizan el derecho fundamental a la protección de datos de carácter personal, regulado por la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 2 Ámbito de aplicación

1. El presente Reglamento será de aplicación a todo tratamiento total o parcialmente automatizado de datos de carácter personal, así como al tratamiento no automatizado de datos de carácter personal incluidos o que vayan a ser incluidos en un fichero no automatizado.

2. Los tratamientos de datos referidos a personas jurídicas no estarán sometidos a lo dispuesto en el presente Reglamento, sin perjuicio de su aplicación al tratamiento de datos de personas físicas que prestan sus servicios o aparezcan relacionados con las mismas.

3. Lo dispuesto en este Reglamento no será de aplicación a los datos referidos a personas fallecidas, sin perjuicio de lo previsto en las Leyes y, en particular, de los derechos reconocidos en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Artículo 3 Ámbito territorial de aplicación

1. Se regirá por el presente Reglamento todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que éste se encuentre ubicado en territorio español.

   Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el Título IV del presente Reglamento.

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.

En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

2. A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Artículo 4. Tratamientos excluidos

El régimen de protección de los datos de carácter personal que se establece en el presente Reglamento no será de aplicación:

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

Sólo se considerarán relacionados con actividades personales o domésticas, los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

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

c) A los tratamientos establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. Sólo tendrán esta consideración aquellos tratamientos respecto de los el responsable del fichero haya comunicado a la Agencia Española de Protección de Datos sus características generales y su finalidad, con carácter previo a su existencia.

Artículo 5. Supuestos especiales

1. Se regirán por sus disposiciones específicas los siguientes tratamientos de datos personales:

a) Los 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, sin perjuicio de las competencias atribuidas a la Agencia Española de Protección de Datos por el artículo 37 m) de la Ley Orgánica 15/1999 y su Estatuto.

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, regulados por el artículo 99 de la Ley 17/1999, de 18 de mayo, de Régimen del Personal de las Fuerzas Armadas.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes, en los términos previstos por sus normas reguladoras.

e) Los regulados por la Ley 4/1997, de 4 de agosto, reguladora de la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

2. Las disposiciones del presente Reglamento serán aplicables supletoriamente a los tratamientos a los que se refiere el apartado anterior, ostentando la Agencia Española de Protección de Datos en relación con los mismos las competencias previstas en el artículo 37.1 de la Ley Orgánica 15/1999.

Artículo 6. Definiciones.

1. A los efectos previstos en este Reglamento, se entenderá por:

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

b) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

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

d) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

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

f) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará responsable del tratamiento a la persona o personas integrantes de los mismos.

g) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la

existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará encargado del tratamiento a la persona o personas integrantes de los mismos.

h) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

i) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará tercero a la persona o personas integrantes de los mismos.

j) 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.

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

l) Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

m) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos .

En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará destinatario a la persona o personas integrantes de los mismos.

n) Transferencia internacional de datos a países terceros: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo , bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

ñ) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español y responsable del tratamiento de los datos de carácter personal que son objeto de transferencia internacional a un país tercero.

o) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

p) Dato disociado: aquél que no permite la identificación de un afectado o interesado .

q) Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

r) Bloqueo: la identificación y reserva de datos de carácter personal con el fin de impedir su tratamiento excepto por parte de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades.

s) Supresión: la eliminación física de los datos de carácter personal bloqueados una vez cumplido el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento durante el cual se guardaron bloqueados.

t) Ficheros de titularidad pública: los ficheros de los que sean responsables los Órganos constitucionales o con relevancia constitucional del Estado o las Instituciones Autonómicas con funciones análogas a las mismas, las Administraciones Públicas Territoriales, las entidades u organismos dependientes de las mismas con personalidad jurídico pública y sometidas al derecho administrativo y las Corporaciones de derecho público, exclusivamente en cuanto dichos ficheros se encuentren estrictamente vinculados al ejercicio de las potestades de derecho público que a las mismas atribuye su normativa específica.

u) Ficheros de titularidad privada: los ficheros de los que sean responsables las entidades sometidas al derecho privado, no vinculados en ningún caso con el ejercicio de potestades de derecho público, incluyendo aquellos de los que sean responsables las fundaciones no sanitarias del sector público, las sociedades del sector público empresarial del Estado, la Comunidad Autónoma, la Provincia o el Municipio, con independencia de su estructura accionarial, y las Corporaciones de Derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de las potestades de derecho público que a las mismas atribuye su normativa específica

2. En particular, en relación con lo dispuesto en el Título IV de este Reglamento se entenderá por:

a) Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

b) Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

b) Recurso: cualquier parte componente de un sistema de información.

c) Usuario: persona, sujeto o proceso autorizado para acceder a datos o recursos.

d) Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

e) Perfil de usuario: accesos autorizados a un grupo de usuarios.

f) Identificación: procedimiento de reconocimiento de la identidad de un usuario.

g) Autenticación: procedimiento de comprobación de la identidad de un usuario.

h) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

i) Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

j) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

k) Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

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

m) Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

n) Copia del respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación

ñ) Documentación: todo escrito, señal, gráfico, sonido, dibujo, película, fotografía, cinta magnética, cinta mecanográfica, cassette, disco, CD-Rom, DVD, dispositivos externos de almacenamiento u otro medio físico en el que se haya registrado información.

o) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

Artículo 7. Fuentes accesibles al público:

1. Sólo tendrán el carácter de fuentes accesibles al público, sin perjuicio de lo dispuesto en el apartado siguiente:

a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999.

b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica

c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los Diarios y Boletines oficiales

e) Los medios de comunicación social.

2. Para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta 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.

TÍTULO II
PRINCIPIOS DE PROTECCIÓN DE DATOS

CAPÍTULO I
CALIDAD DE LOS DATOS

Artículo 8. Principios de calidad de los datos

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

4 Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

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

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, deberán ser rectificados o cancelados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, sin perjuicio de las facultades que a los afectados reconoce el Título III de este Reglamento.

6. 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.

Una vez cumplido el período al que se refiere el párrafo anterior, los datos sólo podrán ser conservados de forma que no permitan la identificación del interesado.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 9. Tratamiento con fines estadísticos, históricos o científicos.

1. No se considerará incompatible, a los efectos previstos en el apartado 4 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

Para la determinación de los fines a los que se refiere el párrafo anterior se estará, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, reguladora de la Función Estadística Pública, la Ley 16/1985, de 25 junio, del Patrimonio Histórico Español y la Ley 13/1986, de 14 de abril de Fomento y Coordinación General de la Investigación Científica y Técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

2. Por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos podrá, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en el Capítulo (xxx) del Título (xxx) del presente Reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

CAPÍTULO II
CONSENTIMIENTO Y DEBER DE INFORMACIÓN

Sección primera
Legitimación para el tratamiento de los datos

Artículo 10. Supuestos que legitiman el tratamiento o cesión de los datos.

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello, en los términos previstos en el presente Reglamento.

2. No obstante, será posible el tratamiento o cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) El tratamiento se lleve a cabo por o la cesión tenga por destinataria una Administración Pública, en los siguiente supuestos:

- Cuando los datos de carácter personal sean recogidos por una Administración Pública en el ámbito de sus competencias.

- Cuando los datos de carácter personal sean cedidos a una Administración Pública en el ámbito de las competencias que le atribuya una norma con rango de Ley o en una norma de derecho comunitario de aplicación directa.

- Cuando el tratamiento se lleve a cabo o la cesión tenga por destinataria una Administración Pública y los datos sean tratados por la misma con fines exclusivamente históricos, estadísticos o científicos.

b) El tratamiento o la cesión se encuentren amparados por una norma con rango de Ley o una norma de derecho comunitario de aplicación directa y en particular:

- Cuando el tratamiento o cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por una norma con rango de Ley o en una norma de derecho comunitario de aplicación directa, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999.

- Cuando el tratamiento o cesión sean necesarios para el cumplimiento de un deber al que se encuentre sujeto en responsable del tratamiento y que esté prevista en una norma con rango de Ley o en una norma de derecho comunitario de aplicación directa.

c) El tratamiento o la cesión se refiera a datos incluidos 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. En este caso, los datos tratados o cedidos deberán ser exclusivamente los contenidos en las fuentes accesibles al público.

d) El tratamiento de los datos se refiera a las partes de un contrato o precontrato, de una relación negocial, laboral o administrativa, por el afectado con el responsable del tratamiento y libremente aceptada por aquél, y sean necesarios para su adecuado mantenimiento, desarrollo o cumplimiento. En este caso el tratamiento sólo será legítimo cuando se limite a la relación jurídica que lo justifique.

e) La comunicación de los datos del afectado sea necesaria para el desarrollo, cumplimiento y control de una relación jurídica, libre y legítimamente aceptada por aquél. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

f) 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 o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la Ley les atribuya expresamente.

Artículo 11. Legitimación para el tratamiento de datos especialmente protegidos.

1. Lo dispuesto en el apartado 2 del artículo anterior no será de aplicación al tratamiento o cesión de los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias de los afectados ni a los relacionados con su origen racial o vida sexual, que se regirán por lo previsto en este artículo.

2. Los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias sólo podrán ser tratados o cedidos previo consentimiento expreso y por escrito de los afectados.

Se exceptúa de lo dispuesto en el párrafo anterior el tratamiento llevado a cabo 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. No obstante, los datos no podrán ser cedidos a terceros sin el previo consentimiento expreso y por escrito del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial 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.

Artículo 12. Legitimación para el tratamiento de datos especialmente protegidos relacionados con la salud.

1. Lo dispuesto en el apartado 2 del artículo 10 no será de aplicación al tratamiento o cesión de los datos de carácter personal relacionados con la salud de los afectados, que se regirán por lo previsto en este artículo.

2. El tratamiento o la cesión de los datos de carácter personal que hagan referencia a la salud de los afectados sólo podrá llevarse a cabo previo el consentimiento expreso del interesado o cuando, por razones de interés general, así se desprenda de lo dispuesto en una Ley o en una norma de derecho comunitario de aplicación directa.

3. En todo caso, los centros sanitarios públicos y privados y los profesionales sanitarios 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 por los mismos, en los términos previstos en la legislación estatal y autonómica en materia de sanidad y en particular en la Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Asimismo, será lícita la cesión de los datos sea necesaria para realizar los estudios epidemiológicos, en los términos establecidos en la legislación estatal o autonómica en materia de sanidad.

Artículo 13. Disposiciones comunes al tratamiento de cualesquiera datos especialmente protegidos

1. No obstante lo dispuesto en los dos artículos anteriores, los datos especialmente protegidos de los afectados podrán ser objeto de tratamiento cuando concurran los requisitos siguientes:

a) resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios; y

b) El tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

2. También podrán ser objeto de tratamiento los datos a que se refiere el apartado anterior cuando el mismo 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 14. Legitimación para el tratamiento de datos relativos a la comisión de infracciones.

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

Sección segunda
Obtención del consentimiento del afectado

Artículo 15. Principios generales.

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en la Ley Orgánica 15/1999 y el presente Reglamento.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y al menos el tipo de actividad desarrollada por el cesionario.

En caso contrario, se considerará que el responsable no ha obtenido el consentimiento del afectado para el tratamiento de sus datos.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado, que no podrá presumirse.

Artículo 16. Forma de recabar el consentimiento.

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 15.2 y 20.1 de este Reglamento y deberá concederle un plazo de 30 días para manifestar su negativa al tratamiento.

En particular, cuando se trate de responsables que presten al afectado un servicio de facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a la facturación del servicio prestado.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y que no implique ingreso alguno para el responsable del tratamiento para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente Reglamento el procedimiento en el que tal negativa pueda efectuarse mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al cliente que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999 los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

5. El responsable del tratamiento no podrá llevar a cabo el tratamiento o cesión al que se refiera la solicitud de consentimiento hasta transcurridos al menos cuarenta y cinco días desde la fecha en que se produjo el envío de la comunicación de solicitud al interesado.

Artículo 17. Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 18. Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, por lo establecido en la presente Sección.

Artículo 19. Revocación del consentimiento.

1. El afectado podrá revocar su consentimiento a través de un medio sencillo y que no implique ingreso alguno para el responsable del tratamiento. A tal efecto, será de aplicación a este supuesto lo establecido en el artículo 16.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999.

El plazo se computará conforme a lo dispuesto en el segundo párrafo del apartado 4 del artículo 29 de este Reglamento.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, el responsable deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en idéntico plazo, para que éstos, a su vez, cesen en el tratamiento de los datos.

Sección tercera
Deber de información al interesado

Artículo 20. Deber de información cuando los datos se recaben directamente del interesado

1. Cuando los datos sean obtenidos del interesado, quien los recabe deberá informarle previamente a dicha recogida y de forma expresa, precisa e inequívoca de:

a) La existencia de un fichero o tratamiento de datos de carácter personal y la incorporación de sus datos al fichero o la realización del tratamiento con los mismos.
b) La identidad y dirección del responsable del fichero o tratamiento o, en su caso, de su representante.
c) La finalidad determinada, explícita y legítima del tratamiento.
d) En su caso, los cesionarios o categorías de cesionarios de los datos, delimitados al menos por el tipo de actividad, determinada y explícita, a la que los mismos se dediquen.
e) El carácter obligatorio o facultativo de la respuesta a las preguntas que le sean planteadas.
f) Las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
g) La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, con indicación de ante quién y de qué modo habrán de ejercitarse.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida de los datos de carácter personal, deberá figurar en los mismos, en forma claramente legible, lo dispuesto en el apartado anterior.

3. La obligación prevista en el apartado 1 no será de aplicación si el interesado ya hubiese sido informado con anterioridad de los extremos contenidos en el mismo.

No será necesaria la información a que se refieren las letras e), f) y g) del apartado 1, si el contenido de la misma se deduce inequívocamente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Artículo 21. Deber de información cuando los datos no se recaben directamente del interesado.

1. 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, de la procedencia de los datos, así como de lo previsto en las letras a), b), c), d) y g) del apartado 1 del artículo anterior, salvo si aquél hubiera ya sido informado con anterioridad.

La obligación prevista en el párrafo anterior deberá cumplirse en el momento en que se produjera la primera cesión de los datos y, en todo caso, dentro de los tres meses siguientes al momento de la recogida.

2. No será de aplicación lo dispuesto en el apartado 1 cuando la cesión o el tratamiento de los datos estén expresamente previstos en una norma con rango de Ley o cuando el tratamiento tenga fines históricos, estadísticos o científicos.

3. Tampoco será de aplicación lo dispuesto en el apartado 1 cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos, que resolverá en cada caso en consideración al número de interesados, a la antigüedad de los datos y a las medidas compensatorias que el responsable del tratamiento se compromete a adoptar.

A tal efecto el responsable del tratamiento deberá solicitar expresamente de la Agencia Española de Protección de Datos la aplicación de la excepción mencionada en el párrafo anterior, justificando la concurrencia de los extremos a los que se refiere el párrafo anterior.

La Agencia Española de Protección de Datos resolverá acerca de la aplicación de la excepción, previa la tramitación del procedimiento previsto en el Capítulo (xxx) del Título (xxx) de este Reglamento.

En la resolución, la Agencia podrá exigir la adopción de medidas compensatorias adicionales o distintas de las propuestas por el responsable del tratamiento.

Artículo 22. Acreditación del cumplimiento del deber de información

El deber de información al que se refieren los artículos anteriores deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

CAPÍTULO IV
ENCARGADO DEL TRATAMIENTO

Artículo 23. Relaciones entre el responsable y el encargado del tratamiento

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. En este caso, el tercero tendrá la condición de encargado del tratamiento.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. El responsable del tratamiento deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. 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.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 24. Requisitos formales para la existencia de un encargado del tratamiento

1. La realización de tratamientos por cuenta del responsable del tratamiento deberá formalizarse a través de un contrato, que deberá revestir forma escrita u otra que acredite su celebración y el contenido mínimo previsto en el apartado siguiente.

2. En el contrato deberá establecerse expresamente que el encargado del tratamiento:

a) Únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento

b) No aplicará o utilizará los datos con un fin distinto al que figure en el contrato

c) No comunicará los datos, ni siquiera para su conservación, a otras personas.

d) Implantará las medidas de seguridad establecidas en el Título IV del presente Reglamento.

Artículo 25. Posibilidad de subcontratación de los servicios

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste poder suficiente para ello. En este caso, la subcontratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de apoderamiento siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y la empresa con la que se vaya a subcontratar.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse

al responsable del tratamiento los extremos los extremos señalados en el apartado anterior.

Artículo 26. Conservación de los datos por el encargado del tratamiento

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

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

TÍTULO III
DERECHOS DE LAS PERSONAS

CAPÍTULO I
DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

Sección Primera
Régimen general

Artículo 27. Carácter personalísimo.

1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado frente al responsable del fichero o tratamiento.

2. Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad frente al responsable, del modo previsto en el artículo siguiente.

b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de

su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél

Artículo 28. Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

2. Deberá concederse al interesado un medio sencillo para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999 y el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la contratación de sus servicios o productos.

5. El responsable del tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Artículo 29.Procedimiento

1. Salvo en el supuesto referido en el párrafo 4 del artículo anterior**,** el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad y, en su caso, de la persona que lo represente , o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica acreditativa de personalidad eximirá de la presentación de las fotocopias del DNI o documento equivalente .

b) Petición en que se concreta la solicitud

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

2. El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

3. En el caso de que la solicitud no reúna los requisitos especificados en el apartado tercero, el responsable del fichero deberá solicitar la subsanación de los mismos.

4. La respuesta deberá cumplir los requisitos de tiempo y contenido previstos para cada caso en el presente Título.

Cuando el plazo para que el responsable del tratamiento haga efectivos los derechos a los que se refiere este Capítulo venga expresado en días, deberá entenderse referido a días hábiles si el responsable es una Administración Pública sometida a lo dispuesto en la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y a días naturales en los demás casos.

5. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.

6. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

Artículo 30. Ejercicio de los derechos ante un encargado del tratamiento

En caso de que existiera un encargado del tratamiento y los afectados solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

Sección Segunda
Derecho de acceso

Artículo 31. Derecho de acceso

1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

2. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.

3 El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 32. Ejercicio del derecho de acceso

1. Al ejercitar el derecho de acceso, el afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la salvaguarda de los derechos de terceros y la configuración o implantación material del fichero o la naturaleza del tratamiento lo permitan:

a) Visualización en pantalla.

b) Escrito, copia o fotocopia remitida por correo, certificado o no.

c) Telecopia.

d) Cualquier otro procedimiento que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable del mismo.

2. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

3. El responsable del fichero deberá cumplir al facilitar el acceso lo establecido en el Título IV de este Reglamento.

Si el responsable del tratamiento ofreciera un determinado procedimiento para hacer efectivo el derecho de acceso y el afectado lo rechazase, serán de cuenta de éste los

posibles riesgos que para la seguridad de la información pudieran derivarse de su elección.

Del mismo modo, si el responsable del tratamiento ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un mayor coste, serán de su cuenta los gastos derivados de su elección.

Artículo 33. Otorgamiento del acceso

1. Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que se refiere el artículo 31.1, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

2. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, y comprenderá todos los datos de base del afectado , los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Artículo 34. Denegación del acceso

1. El responsable del fichero podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.

2. Tratándose de ficheros de titularidad pública podrá también denegarse el acceso en los supuestos previstos en la Ley .

3. Fuera de estos supuestos, el derecho de acceso sólo podrá denegarse cuando exista una norma con rango de Ley o norma de derecho comunitario de aplicación directa que impida al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

4. En todo caso, el responsable del fichero deberá justificar su denegación, con expresión del precepto legal en que se ampare.

Sección Tercera
Derechos de rectificación y cancelación

Artículo 35. Derechos de rectificación y cancelación.

1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

2 El derecho de cancelación es el derecho del afectado a que se bloqueen o supriman los datos que resulten ser inadecuados o excesivos.

En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en el artículo 19 del presente Reglamento.

Artículo 36. Ejercicio de los derechos de rectificación y cancelación

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

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

2. El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

Artículo 37. Denegación de los derechos de rectificación y cancelación.

1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables. Del mismo modo, tampoco procederá la cancelación durante la vigencia de las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

2. Tratándose de ficheros de titularidad pública podrá también denegarse la rectificación o cancelación de los datos en los supuestos previstos en la Ley.

3. Fuera de estos supuestos, los derechos de rectificación y cancelación sólo podrán denegarse cuando exista una norma con rango de Ley o norma comunitaria de aplicación directa que no permita al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el derecho ejercitado.

4. En todo caso, el responsable del fichero deberá justificar su denegación, con expresión del precepto legal en que se ampare.

Artículo 38. Bloqueo de los datos

1. 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.

2. Cumplido el citado plazo deberá procederse a la supresión.

Sección Cuarta
Derecho de oposición

Artículo 39. Derecho de oposición.

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos

a) Cuando no sea necesario su consentimiento para el tratamiento , como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de la publicidad y prospección comercial, en los términos previstos en el artículo 47 de este Reglamento.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión personal automatizada, en los términos previstos en el artículo 41 de este Reglamento.

Artículo 40. Ejercicio del derecho de oposición.

1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento, que deberá ser efectuada en los términos previstos en el artículo 26 del presente Reglamento.

Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

3. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

3. El responsable del fichero deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado segundo de este artículo.

Artículo 41. Derecho de oposición a las decisiones individuales automatizadas

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho. En todo caso, el responsable del fichero deberá informar al afectado de que podrá adoptarse una decisión de las características señaladas en el apartado 1.

b) Esté autorizada por una norma con rango de Ley o norma de derecho comunitario de aplicación directa.

Sección quinta
Del ejercicio de los derechos de acceso, rectificación, cancelación y oposición en relación con ficheros concretos

Subsección Primera
Ficheros del artículo 29 de la Ley Orgánica 15/1999

Artículo 42. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición en los ficheros regulados por el artículo 29.1 de la Ley Orgánica 15/1999.

1. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros regulados por el apartado 1 del artículo 29 de la Ley Orgánica 15/1999 se rige por lo dispuesto en los artículos precedentes del presente Reglamento.

2. Cuando la petición de ejercicio de los derechos se dirigiera al responsable de un fichero de prestación de servicios de solvencia patrimonial y crédito con datos obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento, aquél estará obligado a satisfacer, en cualquier caso, dichos derechos.

3. Si la petición se dirigiera a las personas y entidades a las que se presta el servicio, éstas únicamente estarán obligadas a comunicar al afectado aquellos datos relativos al mismo que les hayan sido comunicados y a facilitar la identidad del responsable.

Artículo 43. Ejercicio de los derechos en los ficheros regulados por el artículo 29.2 de la Ley Orgánica 15/1999.

El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros regulados por el apartado 2 del artículo 29 de la Ley Orgánica 15/1999 se rige por lo dispuesto en los Capítulos I a IV del presente Título, sin perjuicio de lo señalado en los artículos siguientes

Artículo 44. Derecho de acceso en los ficheros del artículo 29.2 de la Ley Orgánica 15/1999

Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, se tendrán en cuenta las siguientes reglas:

1ª. Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.

En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente Reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

2ª. Si la solicitud se dirigiera a cualquier otro participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

Artículo 45. Derecho de rectificación y cancelación en los ficheros del artículo 29.2 de la Ley Orgánica 15/1999

Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, se tendrán en cuenta las siguientes reglas:

1ª. Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de cinco días, procederá a la rectificación o cancelación cautelar de los mismos.

2ª. Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días, dando asimismo respuesta al interesado en los términos previstos en el artículo 36 de este Reglamento.

3ª. Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad del titular del fichero común.

Subsección segunda
Ficheros destinados a la publicidad y prospección comercial.

Artículo 46. Derechos de acceso, rectificación y cancelación.

1. Cuando se ejerciten ante el responsable del fichero destinado a la publicidad y prospección comercial los derechos de acceso, rectificación y cancelación, deberán atenderse los mismos en los términos previstos en los Capítulos I a IV de este Título.

2. Si el derecho se ejercitase ante la entidad beneficiaria de la publicidad, ésta estará obligada a indicar al afectado la identidad del responsable del fichero del que provienen los datos, sin perjuicio del deber impuesto a la misma por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999.

Artículo 47. Derecho de oposición

1. 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.

La oposición a la que se refiere el párrafo anterior deberá entenderse sin perjuicio del derecho del interesado a revocar cuando lo estimase oportuno el consentimiento que hubiera otorgado, en su caso, para el tratamiento de los datos.

2. A tal efecto, deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento. En particular, se considerará cumplido lo dispuesto en este precepto cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico

3. Cuando el responsable del tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999 los supuestos en que el responsable del tratamiento establezca como medio para que el interesado

pueda ejercitar su oposición el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

En todo caso, el ejercicio por el afectado de su derechos no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

4. Cuando el interesado manifieste su deseo de no recibir publicidad, el responsable del fichero podrá conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Subsección Tercera
Historias clínicas

Artículo 48. Ejercicio de los derechos

El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en relación con las historias clínicas se regirá por lo establecido en la Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y en la normativa autonómica reguladora de esta materia.

CAPÍTULO II
OTROS DERECHOS DE LOS AFECTADOS

Artículo 49. Impugnación de valoraciones

1. 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.

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

Artículo 50. 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
DE LAS MEDIDAS DE SEGURIDAD EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CAPÍTULO I
DISPOSICIONES GENERALES

Sección Primera.
Alcance y niveles de seguridad.

Artículo 51. Alcance

1. Los responsables de tratamientos o ficheros que contengan datos de carácter personal, deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 52. Niveles de seguridad.

1. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto.

2. Dichos niveles se establecen atendiendo a la naturaleza de la información tratada y en su caso, de las finalidades de los ficheros o tratamientos de datos de carácter personal en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Artículo 53. Aplicación de los niveles de seguridad.

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico a las que se refiere el Capítulo III del presente Título.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, reguladas por el Capítulo IV de este Título en los siguientes fichero o tratamientos de datos de carácter personal:

- Los relativos a la comisión de infracciones administrativas o penales.
- Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999.
- Aquellos de los que sean responsables las Administraciones Tributarias y se relacionen con el ejercicio de sus potestades tributarias.

- Aquellos de los que sean responsables las entidades financieras y para finalidades relacionadas con la prestación de servicios financieros.
- Aquellos que contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.
- Aquellos que contengan datos relativos a menores de 14 años y a víctimas de violencia de género.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto reguladas en el Capítulo V de este Título se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

- Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- Aquellos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico o localización.
- Los que contengan datos y claves necesarios para emitir certificados digitales que permitan realizar firma electrónica excepto aquellos que por su propia naturaleza deban ser públicos.

Los ficheros o tratamientos relativos a ideología, afiliación sindical, religión o creencias, así como a la salud, cuya finalidad sea únicamente la gestión de obligaciones por el retenedor o la transferencia dineraria a las entidades de las que los afectados sean asociados o miembros, podrán adoptar respecto de aquellos las medidas de seguridad de nivel básico.

4. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

Artículo 54. Encargado de tratamiento

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos a un encargado de tratamiento preste sus servicios en los locales del responsable del tratamiento deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal sujeto a la dirección del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en locales ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas para dicho tratamiento en este Reglamento.

Artículo 55. Otras prestaciones de servicios sin acceso a datos personales

En relación con el personal propio o ajeno con acceso físico a los locales en los que se encuentran los ficheros o tratamientos de datos personales para la realización de trabajos que no impliquen el tratamiento de datos personales, como los servicios de limpieza o de mantenimiento, el responsable del fichero adoptará las medidas adecuadas para limitar el acceso de estas personas a los datos personales y recogerá en el contrato de prestación de servicios cláusulas relativas a la prohibición de acceder a los datos personales y a la obligación de secreto respecto a los datos a los que, en la prestación del servicio, el personal hubiera podido conocer.

Artículo 56. Delegación de autorizaciones

Las autorizaciones que en este Título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 57. Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 53.

Artículo 58. Régimen de trabajo fuera de los locales del responsable del fichero o encargado de tratamiento.

1. Cuando los datos personales se almacenan en dispositivos portátiles o se tratan fuera de los locales del responsable de fichero será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 59. Ficheros temporales o copias de trabajo de documentos.

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Reglamento.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II
DEL DOCUMENTO DE SEGURIDAD

Artículo 60. El documento de seguridad

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnico y organizativo acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los ficheros o tratamientos de datos de carácter personal.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

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

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos , así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de éstos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio previstas en este Título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. El documento de seguridad deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado en su organización o en el contenido de la información incluida en los ficheros o tratamientos.

6. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPÍTULO III
MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Sección Primera
Medidas generales

Artículo 61. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada una de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 62. Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 63. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos..

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 64. Gestión de soportes y documentos

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad. Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento.

2. La salida de soportes y documentos que contengan datos de carácter personal, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por éste.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Sección Segunda
Medidas aplicables a los ficheros automatizados

Artículo 65. Identificación y autenticación.

1. El responsable del fichero deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios. Para ello podrán utilizarse mecanismos basados en certificados digitales electrónicos.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la autenticación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad con la que tienen que ser cambiadas las contraseñas, y mientras estén vigentes se almacenarán de forma ininteligible.

Artículo 66.Copias de respaldo y recuperación.

1. El responsable de fichero se encargará de verificar la correcta definición, pruebas de funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. En todo caso, cada 6 meses deberá realizarse la verificación prevista en el apartado 1.

Sección Tercera
Medidas aplicables a los ficheros no automatizados

Artículo 67. Almacenamiento de la información

Los soportes de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

Igualmente, se deberá identificar el tipo de información que contienen, ser inventariados y almacenarse en lugares controlados por el personal autorizado para ello en el documento de seguridad.

Artículo 68. Criterios de archivo.

El responsable del fichero deberá establecer los procedimientos que deban seguirse en el archivo de los ficheros no automatizados. Dichos procedimientos estarán dirigidos a garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de acceso, oposición, rectificación y cancelación.

CAPÍTULO IV
MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Sección Primera
Medidas generales

Artículo 69. Responsable de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento.

Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

Artículo 70. Registro de accesos.

1. De cada acceso se guardarán, como mínimo, 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.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

6. No será necesario el registro de accesos definido en este artículo siempre y cuando el responsable del fichero o tratamiento garantice que sólo él tiene acceso y trata los datos personales. Esta circunstancia deberá hacerse constar motivadamente en el documento de seguridad.

Artículo 71. Auditoria.

1. Los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán a una auditoria interna o externa, que verifique el cumplimiento del

presente Título, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

2. El informe de auditoria deberá dictaminar sobre la adecuación de las medidas y controles al presente Título, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoria serán entregados al responsable del fichero o tratamiento y al responsable de seguridad para que se adopten las medidas correctoras adecuadas y quedará a disposición de la Agencia Española de Protección de Datos, a la que además notificará la fecha del informe y la indicación de si se trata de un auditor interno o externo.

Artículo 72. Gestión de documentos y soportes.

1. Deberá establecerse un sistema de registro de entrada de soportes informáticos y de documentos que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos y de documentos que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Sección Segunda
Medidas aplicables a los ficheros automatizados

Artículo 73. Identificación y autenticación.

1. El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 74. Control de acceso físico

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Artículo 75. Registro de incidencias.

1. En el registro regulado en el artículo 62 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Artículo 76. Pruebas con datos reales.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado.

Artículo 77. Régimen de trabajo fuera de los locales del responsable del fichero o encargado de tratamiento.

Cuando los datos personales se almacenan en dispositivos portátiles o se tratan fuera de los locales del responsable de fichero será preciso que se proceda al cifrado de los mismos.

Sección Tercera
Medidas aplicables a los ficheros no automatizados

Artículo 78. Seguridad en los locales de ubicación de los ficheros.

El lugar en que se encuentre el fichero deberá estar dotado de mecanismos que impidan la posible destrucción o que no sea posible la recuperación de la información, tales como dispositivos ignífugos, equipamiento contra incendios y otros similares.

Artículo 79. Acceso físico.

1. Los armarios, archivadores u otros elementos en los que se almacenen datos de carácter personal deberán encontrarse ubicados en áreas o salas en las que el acceso esté restringido única y exclusivamente al personal autorizado en el Documento de Seguridad.

No obstante, si las características físicas de los locales de que dispusiera el responsable del tratamiento no permiten cumplir lo previsto en el párrafo anterior, dichos elementos de almacenamiento deberán estar ubicados en lugares que estén bajo vigilancia del personal autorizado en el documento de seguridad, y estar dotados de mecanismos que impidan el libre acceso a los mismos por parte de personas no autorizadas.

En el documento de seguridad deberán constar motivadamente las circunstancias que impidan el cumplimiento de esta medida.

2. Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los armarios, archivadores u otros elementos o soportes en los que se almacenen los datos de carácter personal.

Artículo 80. Copia o reproducción

1. Deberán establecerse procedimientos en el copiado o reproducción de documentos, a fin de que sólo puedan realizar copias de documentos o acceder a las mismas las personas habilitadas para ello en el documento de seguridad.

2. El responsable del fichero o tratamiento arbitrará los controles necesarios para evitar que como consecuencia de la generación de copias se produzcan accesos no autorizados. Dichos controles deberán recogerse en el documento de seguridad.

CAPÍTULO V
MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Sección Primera
Medidas generales

Artículo 81. Distribución de soportes.

La distribución de los soportes y documentos que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Así mismo, se cifraran los datos que contenga los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones bajo el control del responsable del fichero.

Sección Segunda
Medidas aplicables a los ficheros automatizados

Artículo 82. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan , que deberá cumplir en todo caso las medidas de seguridad exigidas en este Título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 83. Telecomunicaciones.

La transmisión de datos de carácter personal a través de redes públicas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Sección Tercera
Medidas aplicables a los ficheros no automatizados

Artículo 84. Registro de accesos.

1. Cualquier solicitud de acceso a los documentos incluidos en un fichero no automatizado deberá efectuarse a la persona o personas designadas a tal efecto en el documento de seguridad.

2. Deberá existir un registro de accesos autorizados en el que se indicará como mínimo el documento al que se ha accedido, la fecha y hora del acceso, y la fecha y hora de la devolución.

3. El período mínimo de conservación de la información recogida en el registro al que se refiere el párrafo anterior será dedos años. El responsable de seguridad revisará periódicamente la información registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos cada dos meses.

4. La documentación se reintegrará al fichero tan pronto haya cesado el motivo que justificó el acceso y se controlará la devolución.

Artículo 85. Almacenamiento de la información

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

2. Si atendidas las características de los locales de que dispusiera el responsable del tratamiento no fuera posible cumplir lo establecido en el apartado anterior, el responsable de seguridad elaborará un informe motivado sobre esta circunstancia que elevará al responsable del fichero junto con una propuesta de soluciones alternativas. En todo caso los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse dotados de sistemas que obstaculicen el acceso no autorizado a los mismos. Dichos sistemas deberán permanecer activados en tanto no sea precisa su apertura.

3. Mientras la documentación con datos de carácter personal no se encuentre archivada en el lugar de almacenamiento establecido en el apartado 1 por estar en proceso de

revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Artículo 86. Traslado de documentación

Siempre que se proceda la traslado de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado y controles que permitan detectar si se ha producido algún acceso no autorizado.

Artículo 87. Copia o reproducción

La utilización de la copia estará sometida a las medidas descritas en la presente Sección.

TÍTULO VIII
TRANSFERENCIAS INTERNACIONALES DE DATOS

CAPÍTULO I
DISPOSICIÓN GENERAL

Artículo 88. Cumplimiento de las disposiciones de la Ley Orgánica 15/1999.

La transferencia internacional de datos no excluye en ningún caso la aplicación de las restantes disposiciones contenidas en la Ley Orgánica 15/1999 y en el presente Reglamento.

Artículo 89. Autorización y notificación

1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999 y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 120 del presente Reglamento.

La autorización se otorgará conforme al procedimiento establecido en el Capítulo (xxx) del Título (xxx) de este Reglamento.

2. La autorización no será necesaria:

a) Cuando el estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el Capítulo II de este Título.

b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en el artículo 94 de este Reglamento.

3. En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos

CAPÍTULO II
TRANSFERENCIAS AL TERRITORIO DE ESTADOS QUE OTORGUEN UN NIVEL ADECUADO DE PROTECCIÓN

Artículo 90. Nivel adecuado de protección declarado por la Agencia Española de Protección de Datos.

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará 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

2. Mediante Resolución del Director de la Agencia Española de Protección de Datos podrá publicarse la relación de países que se considera que proporcionan un nivel de protección adecuado, a efectos de lo dispuesto en este artículo.

Artículo 91. Nivel adecuado de protección declarado por Decisión de la Comisión Europea.

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

Artículo 92. Suspensión temporal de las transferencias

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37 f) de la Ley Orgánica 15/1999, podrá acordar, previa audiencia del exportador , la suspensión

temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a) Que las Autoridades de Protección de Datos del Estado importador o cualquier otra, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos de su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea.

CAPÍTULO III
TRANSFERENCIAS AL TERRITORIO DE ESTADOS QUE NO OTORGAN UN NIVEL ADECUADO DE PROTECCIÓN

Artículo 93. Transferencias sujetas a autorización del Director de la Agencia Española de Protección de Datos.

1. Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se aprecie por el Director de la Agencia Española de Protección de Datos la existencia de un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

2. La autorización será otorgada en caso de que el responsable del fichero aporte un contrato escrito, celebrado entre el exportador y el importador , en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

A tal efecto, se considerará que establecen las adecuadas garantías los contratos se celebrasen al amparo de lo que establecen las Decisiones de la Comisión Europea e la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, y 2002/16/CE, de 27 de diciembre de 2001, o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

3. En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37 f) de la Ley Orgánica 15/1999, suspender temporalmente, previa audiencia

del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

4. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos códigos de conducta en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el ejercicio por éstos de los derechos reconocidos en la Ley Orgánica 15/1999 y el presente Reglamento.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas contenidas en el código resulten vinculantes para las empresas del Grupo y las mismas puedan ser debidamente ejecutadas conforme al derecho español.

5. La autorización de la transferencia se tramitará conforme al procedimiento establecido en el Capítulo (xxx) del Título (xxx) del presente Reglamento.

Artículo 94. Transferencias no sujetas a autorización del Director de la Agencia Española de Protección de Datos.

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de las transferencias internacionales de datos que tuvieran por importador una persona física o jurídica, pública o privada, situada en el territorio de un Estado respecto del que no se haya declarado por la Comisión Europea o no se aprecie por el Director de la Agencia Española de Protección de Datos la existencia de un nivel adecuado de protección en caso de que el exportador fundamente la transferencia en alguno de los siguientes supuestos:

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.