La Seguridad Informática y la Protección de los Datos de Carácter Personal en las Entidades Locales

DEPUTACIÓN PROVINCIAL DE OURENSE

Manual de Aplicación de la "Ley Orgánica de Protección de Datos" en la Administración Local

Deputación de Ourense • Negociado de Formación

Álvaro Gómez Vieites

Es Ingeniero de Telecomunicación por la Universidad de Vigo, habiendo cursado las dos especialidades de Telemática y de Comunicaciones, obteniendo el número uno de su promoción (1996) y Premio Extraordinario Fin de Carrera. Su formación se ha completado con varios cursos programas de postgrado, entre ellos el *Executive MBA* y el *Diploma in Business Administration* de la Escuela de Negocios Caixanova. Ha sido Director de Sistemas de Información y Control de Gestión en la Escuela de Negocios Caixanova. En la actualidad, es profesor colaborador de esta entidad, actividad que compagina con la consultoría en las empresas SIMCe, EOSA y EDISA, contando con una amplia experiencia organizando seminarios para directivos en el área de Internet y el impacto de las Tecnologías de la Información en la empresa.

La Seguridad Informática y la Protección de los Datos de Carácter Personal en las Entidades Locales

Manual de Aplicación de la "Ley Orgánica de Protección de Datos" en la Administración Local

Álvaro Gómez Vieites

La Diputación Provincial de Ourense afronta la edición de esta publicación sobre "La seguridad informática y la protección de los datos de carácter personal" como un servicio público de notable utilidad para las entidades locales, especialmente para los pequeños municipios.

Con esta ley, las administraciones públicas asumimos una serie de responsabilidades en la custodia de datos personales que no siempre son conocidas en detalle y en este libro tratamos de ofrecer una visión general del procedimiento a seguir, así como información en materia legislativa o de órganos de control y asesoramiento a los que recurrir.

Nuestro deseo es que este libro sea para todos ustedes una herramienta útil y eficaz, pues nace claramente con una vocación de servicio al ciudadano, a través de sus administraciones.

José Luis Baltar Pumar

Presidente de la Diputación de Ourense

ÍNDICE

Capítulo 1

1. Derecho a la Intimidad y a la Privacidad

Podemos definir el **Derecho a la Intimidad y a la Privacidad** como el derecho que poseen las personas de poder excluir a terceros del conocimiento de su vida personal, es decir, de sus sentimientos, sus emociones, sus datos biográficos y personales y su propia imagen.

Asimismo, algunos juristas también hablan de la facultad de determinar en qué medida esas dimensiones de la vida personal de un ciudadano pueden ser legítimamente comunicadas o conocidas por otras personas. En este sentido, se trataría de establecer el derecho de un individuo al control sobre quién, cuándo y dónde se podrían percibir diferentes aspectos de su vida personal (a través de sus datos personales).

La propia Declaración Universal de Derechos Humanos del año 1948, en su artículo 12, establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

En el ámbito de la Unión Europea la nueva Constitución Europea considera el derecho a la protección de los datos personales como un derecho fundamental, independientemente de que exista o no un tratamiento informatizado de estos datos.

De hecho, el artículo II-68 de la Constitución Europea se dedica íntegramente al Derecho a la Protección de Datos de Carácter Personal, estableciendo que:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

Tabla 1: *Artículo II-68 de la Constitución Europea*

Sin embargo, en estos últimos años, a raíz de la amenaza del terrorismo internacional, estamos asistiendo a un recorte de estas libertades de los ciudadanos en los países occidentales. En Estados Unidos, la polémica ley antiterrorista "*Patriot Act*" (la Ley Patriota), aprobada por el Congreso estadounidense un mes después de los atentados terroristas del 11 de septiembre de 2001, ha recibido numerosas críticas por parte de grupos defensores de los derechos civiles y algunos políticos, al considerar que esta Ley va demasiado lejos y viola las libertades fundamentales de los individuos.

De hecho, esta ley antiterrorista de Estados Unidos expande los poderes policiales, permite las escuchas telefónicas sin una razón específica y da vía libre a la vigilancia de los estadounidenses en todos los sitios públicos, permitiendo incluso a la policía federal revisar los libros que una persona solicita en una biblioteca o los vídeos que alquila (situación de la que se informa a los ciudadanos mediante carteles informativos ubicados en estos centros públicos). También restringe los actos de protesta y de desobediencia civil en contra de las políticas del Gobierno de Estados Unidos.

Por todos estos motivos, varios Estados y más de un centenar de ciudades y condados de Estados Unidos han aprobado resoluciones de repulsa a la "*Patriot Act*", en las que se pide que se anulen aquellas normas que violen los derechos y libertades garantizados por la Constitución estadounidense.

En septiembre de 2004 un juez federal de Nueva York declaró anticonstitucional una parte de la "*Patriot Act*", en respuesta a una demanda de la Unión Estadounidense de Libertades Civiles, que desafió en abril de 2004 los amplios poderes otorgados por esa polémica ley al FBI. El juez se refiere en su decisión al capítulo de la ley que permitía a los agentes de la Oficina Federal de Investigaciones (FBI) exigir a los proveedores de Internet y a otras empresas información confidencial sobre sus clientes dentro de sus investigaciones sobre terrorismo, sin aprobación judicial y sin necesidad de demostrar una necesidad imperiosa que justificara el acceso a los documentos.

Sin embargo, el gobierno de Estados Unidos ha continuado poniendo en marcha medidas para controlar las actividades de sus ciudadanos, hasta el extremo de que a finales de 2005 el Departamento de Justicia solicitaba a los principales portales y buscadores de ese país que le facilitasen información acerca de cuáles eran los términos de búsqueda de sus usuarios. Algunos buscadores como Google se negaron a facilitar estos datos a la Administración Bush, iniciando de este modo un enfrentamiento ante los tribunales, al entender que esta medida atentaba contra el derecho a la intimidad de sus usuarios.

También se está planteando esta restricción de las libertades en Europa. A raíz de los atentados terroristas de Madrid (11 de marzo de 2004) y, especialmente, de Londres (7 de julio de 2005), distintos gobiernos europeos liderados por el británico se han mostrado partidarios de facilitar el acceso de la Policía a las llamadas telefónicas y los correos electrónicos de los ciudadanos.

De hecho, en el Parlamento Europeo se ha planteado la polémica medida de obligar a los operadores de telecomunicaciones a retener durante 12 meses estos datos (con el importante coste económico que conlleva poner en marcha esta medida). A finales de noviembre de 2005 el Comité de Libertades Civiles del Parlamento de la Unión Europea votaba mayoritariamente a favor de registrar los datos de todas las llamadas telefónicas y del uso de Internet en los Estados miembros de la Unión durante un período de seis meses a un año para ayudar a combatir el terrorismo y otros delitos. La nueva Directiva Europea sobre retención de datos telefónicos y de comunicaciones electrónicas era finalmente aprobada por el Parlamento Europeo el 15 de diciembre de 2005.

Esta medida constituye un paso inédito en algunos países en los cuales, como en el caso del Reino Unido, los derechos a la intimidad y la libertad individual se consideraban preciados tesoros, hasta el extremo de que sus ciudadanos no tenían documento nacional de identidad.

Sin embargo, estas medidas de control de las llamadas se están encontrando con el problema de la interceptación de las cada vez más numerosas llamadas telefónicas que realizan los ciudadanos a través de servicios como SKYPE, recurriendo a la telefonía IP, donde los datos de cada conversación se envían encriptados a través de Internet. De este modo, la voz IP no sólo permite abaratar de forma drástica los costes de las comunicaciones, sino que incluso garantiza en este momento una mayor protección de la privacidad de sus usuarios.

Por su parte, Francia está preparando un proyecto de Ley que contempla nuevas medidas en la lucha contra el terrorismo, entre las que destaca la obligación impuesta a todos los cibercafés para que conserven los datos técnicos de todas las conexiones de sus clientes, incluidos los proveedores de acceso a Internet utilizados, los números de teléfono entrantes y salientes, las direcciones a las que se conectan y los enlaces con teléfonos móviles, con el fin de que puedan ser consultados por la policía antiterrorista.

En España, desde el mes de octubre de 2005 varias compañías aéreas como Iberia han comenzado a suministrar datos sobre sus pasajeros al Ministerio del Interior, dentro de las medidas que este departamento ha puesto en marcha en su plan de lucha contra el terrorismo islamista y en aplicación de las recomendaciones de la comisión de investigación del 11-M[1].

[1] Atentado terrorista de Madrid del 11 de marzo de 2004.

Capítulo 2

2. Cómo garantizar la protección de datos personales y la privacidad

La protección de los datos personales y de la privacidad es una cuestión que genera bastante polémica en la actualidad, debido a que existen posturas manifiestamente encontradas, a pesar de que este derecho fundamental de todo ciudadano ya había sido reconocido en la Declaración Universal de los Derechos Humanos de 1948.

Así, por una parte, un grupo de países liderados por la Unión Europea son partidarios de una estricta regulación estatal, con fuertes sanciones para aquellas organizaciones que incumplan las normas establecidas (postura conocida como "*hardlaw*"). También en muchos países de Latinoamérica se ha reconocido el derecho fundamental a la protección de los datos personales de los ciudadanos.

Por otra parte, otros países como Estados Unidos son mucho más permisivos con las actuaciones de las empresas, y abogan por una autorregulación y la elaboración de códigos éticos de conducta, sin la intervención por parte de los Estados (postura conocida como "*softlaw*"). Habría que tener en cuenta, además, las fuertes presiones de las empresas y ciertos grupos de poder para impedir la intervención estatal sobre esta cuestión.

De hecho, en Estados Unidos son perfectamente legales servicios de venta de datos personales como "US Search" (www.ussearch.com), que permiten acceder a informes con datos de carácter personal de todo tipo, obtenidos de fuentes y bases de datos de las propias Administraciones Públicas y de empresas privadas: Administraciones de Justicia y Militares, registros de comercio, oficinas de patentes, bases de datos de abonados a televisión por cable, suscriptores de

periódicos, registros de las prisiones (en los Estados que lo autorizan), registros de adopción (en los Estados que lo autorizan), registro de delincuentes sexuales (en los Estados que lo autorizan), depósitos de cadáveres, etc.

Figura 1: US Search (www.ussearch.com)

De este modo, por apenas 40 dólares es posible adquirir a través de su página Web un informe personal sobre un determinado ciudadano (teniendo que facilitar para ello el nombre y la edad aproximada de esta persona), en el que se incluyen datos como los siguientes:

- Direcciones conocidas en los últimos 10 años.
- Números de teléfono que tuvo registrados a su nombre.
- Nombres de familiares más cercanos, sus cónyuges o las personas que se encuentran empadronadas en la misma vivienda.
- Nombre de sus posibles vecinos.
- Direcciones de sus propiedades registradas y su valor catastral.
- Bienes y otras propiedades a su nombre.
- Licencias profesionales que posee.

- Sentencias civiles o criminales en las que figure (permite conocer el historial de cargos y condenas, estancias en la cárcel, etc.).
- Quiebras en las que se encuentre involucrado.
- Etc.

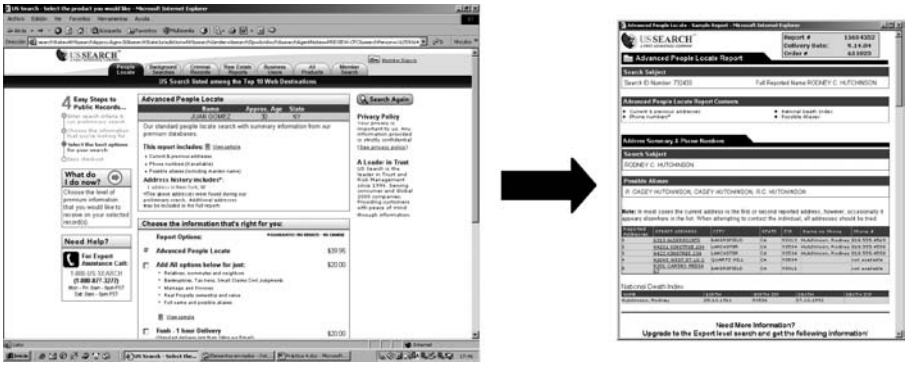
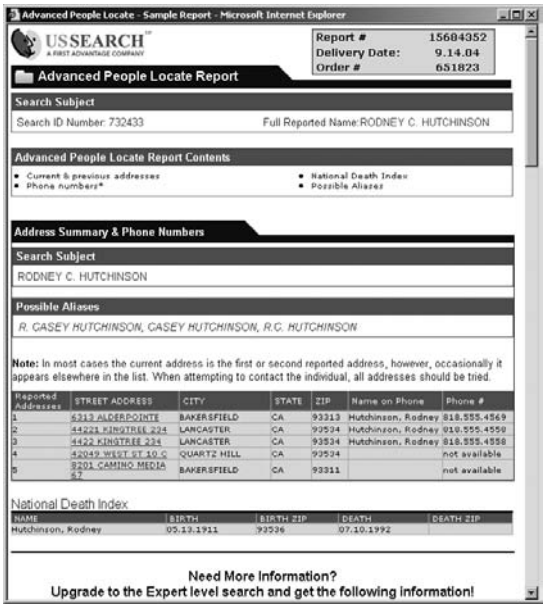


Figura 2: Compra de un informe en "US Search"



Advanced People Locate - Sample Report - Microsoft Internet Explorer

USSEARCH
A FIRST ADVANTAGE COMPANY

Report # 15684352
Delivery Date: 9.14.04
Order # 651823

Advanced People Locate Report

Search Subject

Search ID Number: 732433 Full Reported Name:RODNEY C. HUTCHINSON

Advanced People Locate Report Contents

- Current & previous addresses
- Phone numbers*
- National Death Index
- Possible Aliases

Address Summary & Phone Numbers

Search Subject

RODNEY C. HUTCHINSON

Possible Aliases

R. CASEY HUTCHINSON, CASEY HUTCHINSON, R.C. HUTCHINSON

Note: In most cases the current address is the first or second reported address, however, occasionally it appears elsewhere in the list. When attempting to contact the individual, all addresses should be tried.

Reported Addresses	STREET ADDRESS	CITY	STATE	ZIP	Name on Phone	Phone #
1	4313 ALDERPOINTE	BAKERSFIELD	CA	93313	Hutchinson, Rodney	818.555.4569
2	44221 KINGTREE 224	LANCASTER	CA	93534	Hutchinson, Rodney	818.555.4559
3	4422 KINGTREE 224	LANCASTER	CA	93534	Hutchinson, Rodney	818.555.4558
4	42049 WEST ST 10 C	QUARTZ HILL	CA	93534		not available
5	8201 CAMINO MEDIA 67	BAKERSFIELD	CA	93311		not available

National Death Index

NAME	BIRTH	BIRTH ZIP	DEATH	DEATH ZIP
Hutchinson, Rodney	05.13.1911	93536	07.10.1992	

Need More Information?
Upgrade to the Expert level search and get the following information!

Figura 3: Ejemplo de informe de "US Search"

Por lo tanto, los clientes de "US Search" podrían fácilmente obtener respuestas a preguntas del tipo:

- ¿Tiene el vecino antecedentes penales?
- ¿Está involucrado mi nuevo compañero de trabajo en una quiebra?
- ¿Dónde han vivido durante los últimos años los padres del nuevo amigo de mis hijos y qué propiedades tienen?
- ¿Con quién ha estado casada la nueva niñera de mis hijos, quiénes son sus familiares y dónde ha vivido en los últimos 10 años?

Tras suministrar la información, "*US Search*" advierte a su cliente que "a la persona buscada no se le notificará que usted la busca y, en consecuencia, le rogamos que actúe de forma responsable de acuerdo con la legislación vigente". Sin embargo, ofrece a sus clientes, por una tarifa anual, la contratación del servicio para recibir información acerca de quién puede estar preguntando por ellos y qué datos han podido obtener.

De un modo similar, en estos últimos tiempos se han popularizado en Estados Unidos los servicios que publican a través de Internet los datos personales y las deudas que han dejado pendientes de pago las personas morosas, como medida de presión para que resuelvan su situación de morosidad cuanto antes.

La situación es totalmente distinta en Europa, donde se ha definido un estricto marco legal, con elevadas sanciones para las empresas, las Administraciones Públicas e incluso los propios ciudadanos que lo puedan incumplir a nivel particular.

En la Unión Europea este marco normativo viene determinado por la Directiva 95/46/CE del Parlamento Europeo, relativa a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales y la libre circulación de éstos por parte de empresas, Administraciones Públicas y ciudadanos de la Unión Europea.

De este modo, los gobiernos europeos se muestran claramente decididos a promover la cultura de la protección de datos entre las Administraciones Públicas y las empresas, estableciendo además la existencia de autoridades independientes de control (como las Agencias de Protección de Datos en España), con funciones ejecutivas (registro de ficheros, control, inspección y sanción), funciones normativas y de carácter consultivo, como garantes del respeto de este derecho fundamental en los Estados miembros de la Unión Europea.

Por su parte, en España el artículo 18.4 de la Constitución ya contempla que el Estado debe limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. La publicación de la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (LOPD), define el marco legal de la protección de los datos de carácter personal en el Estado español.

En definitiva, esta situación con dos posturas claramente enfrentadas ha provocado en los últimos años fuertes tensiones entre Estados Unidos y la Unión Europea, sobre todo desde la aprobación de la directiva 95/46/CE del Parlamento Europeo, que entró en vigor en octubre de 1998, impidiendo expresamente la cesión de datos personales a empresas de otros países que, como Estados Unidos, no dispongan de unas normas equivalentes.

2.1. *Acuerdo entre la Unión Europea y Estados Unidos sobre protección de datos.*

Tras más de dos años de duras negociaciones, que estuvieron a punto de provocar una guerra comercial con sanciones por ambas partes, finalmente la Comisión Europea dio luz verde en marzo de 2000 al comisario de Mercado Interior para que aceptase las garantías propuestas por Estados Unidos en materia de protección de datos de carácter personal, a través del principio denominado como "*safe harbor*" ("puerto seguro").

En virtud de este acuerdo, las empresas estadounidenses interesadas en figurar en la lista "*safe harbor*" podrán inscribirse de forma voluntaria, estando obligadas entonces a otorgar a los datos de los clientes un nivel de protección similar al existente en Europa. Así, por ejemplo, no podrán comercializar estos datos sin consentimiento previo de los interesados y éstos tendrán derecho a ser informados acerca de qué datos figuran en los ficheros informáticos de estas empresas. La violación de estos códigos de conducta voluntarios conlleva responsabilidad penal en Estados Unidos.

De este modo, los ciudadanos y las empresas europeas podrán decidir si entablan relaciones comerciales con empresas de Estados Unidos en las que sea necesario comunicar datos de carácter personal.

Se puede consultar la lista de entidades estadounidenses adheridas a los principios de "Puerto Seguro" en la página Web del Departamento de Comercio de Estados Unidos: www.export.gov/safeharbor

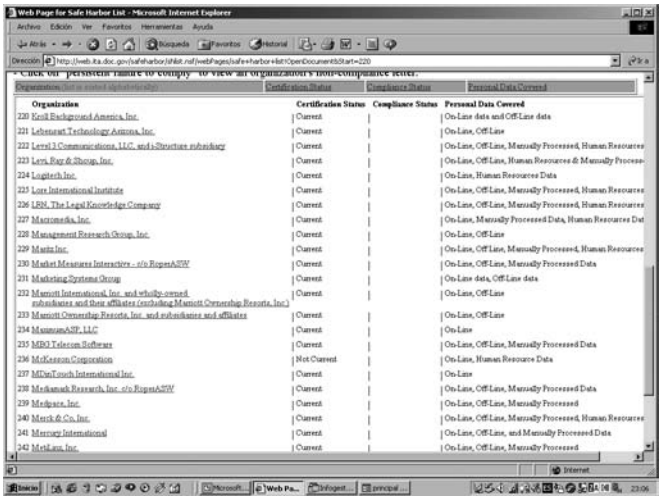


Figura 4: *Lista "Safe Harbor"*

Sin embargo, más recientemente ha surgido un nuevo punto de conflicto en la Unión Europea y Estados Unidos, a raíz de la obligación impuesta por Estados Unidos a las compañías aéreas de entregar las listas con los datos personales de los pasajeros embarcados y de las tripulaciones de vuelos con origen, destino o escala en un aeropuerto de ese país.

De este modo, como consecuencia de la aplicación de la Ley de Seguridad en los Transportes de Estados Unidos, las compañías aéreas deben facilitar un acceso electrónico a los datos de sus pasajeros al Servicio de Aduanas y Protección de Fronteras (datos incluidos en la lista PNR, "*Passenger Names Register*"), bajo la amenaza de fuertes sanciones e incluso de la pérdida de los derechos de aterrizaje si se niegan a colaborar con las autoridades estadounidenses.

En diciembre de 2003 la Comisión Europea alcanzó un acuerdo con la Administración estadounidense, tras considerar que el Servicio de Aduanas y Protección de Fronteras de Estados Unidos (CBP) garantizaba un nivel de protección adecuado para estos datos personales de ciudadanos europeos. Este acuerdo era aprobado por el Consejo de la Unión el 17 de mayo de 2004.

Seguidamente se presentan los principales puntos del acuerdo con el Servicio de Aduanas de Estados Unidos:

- Las autoridades estadounidenses capturarán y conservarán menos datos de los inicialmente previstos.
- Los datos sensibles, como las preferencias alimentarias o las necesidades especiales de los pasajeros, que pueden revelar su raza, religión o estado de salud, no se transferirán o, si se transfieren, serán filtrados y eliminados por el Servicio de Aduanas de Estados Unidos.
- Los datos de los pasajeros se utilizarán exclusivamente para prevenir y combatir el terrorismo y los delitos conexos, así como otros delitos graves, incluida la delincuencia organizada, que tengan carácter transnacional.
- Los datos de los pasajeros no se compartirán "en masa" con otros organismos del gobierno de Estados Unidos. El Servicio de Aduanas compartirá los datos de los pasajeros de forma limitada, caso por caso, y únicamente para las finalidades acordadas.
- La mayoría de los datos de los pasajeros serán suprimidos al cabo de tres años y medio, frente a los cincuenta años que proponían en un principio las autoridades de Estados Unidos.

Cabe destacar que Japón ha decidido adoptar medidas similares a las de Estados Unidos. Así, a principios de 2005 las autoridades japonesas ponían en marcha el "Sistema Avanzado de Información sobre Pasajeros", para conocer de antemano y archivar en fichas la identidad de pasajeros aéreos que llegan a Japón. Este sistema pretende reforzar la seguridad contra el terrorismo y prevenir las entradas de ilegales a este país, además de ayudar a frenar el contrabando y el tráfico de drogas.

Por este motivo, las aerolíneas de vuelos internacionales con destino a Japón deberán facilitar los datos personales recogidos en el momento del abordaje, como el nombre, nacionalidad, sexo y número de pasaporte. Esta

información será contrastada con una base de datos conjunta de la policía, la inmigración y la aduana japonesas para confirmar la presencia de individuos sospechosos en los vuelos.

2.2. Legislación sobre protección de datos en Estados Unidos.

A pesar de que no existe una ley específica sobre protección de datos de carácter personal, sí es cierto que en Estados Unidos se han aprobado leyes para regular y proteger los datos de carácter personal en determinadas circunstancias y actividades.

Así, por ejemplo, en el ámbito de la salud de las personas, la "*Health Insurance Portability and Accountability Act*" (HIPAA) es una Ley Federal de 1996 que controla el almacenamiento y transmisión electrónica de los datos personales de los pacientes de clínicas y hospitales. Esta Ley exige que los médicos y profesionales de la salud cumplan con unos mínimos estándares de seguridad informática e informen a sus pacientes sobre las medidas de seguridad adoptadas, además de documentar cualquier cesión de datos de sus pacientes a entidades externas (salvo en algunas excepciones).

Todas las prácticas médicas en Estados Unidos deben cumplir con lo establecido en la HIPAA desde abril de 2003. Se contemplan multas de hasta 250.000 dólares y de 10 años de prisión para las violaciones más graves de la ley: divulgación deliberada de la información de los pacientes con la intención de venderla, transferirla o utilizarla con ánimo de lucro personal o comercial o con fines malintencionados, etc.

En el ámbito financiero podemos citar la "*Gramm-Leach-Bliley Act*" (GLB Act), una Ley Federal de 1999 que impone una serie de restricciones a las entidades financieras en relación con la protección, utilización y cesión de los datos personales de sus clientes, con el objetivo fundamental de garantizar la confidencialidad e integridad de los datos de los clientes y evitar accesos no autorizados a estos datos.

En lo que se refiere a la protección de los menores de edad, la "*Children's Online Privacy Protection Act*" es una Ley Federal que entró en vigor en abril de 2000, imponiendo una serie de restricciones a la captura de datos personales de los niños menores de 13 años que se conectan a páginas Web y a otros servicios de Internet.

Por otra parte, ante los continuos problemas de seguridad en muchas empresas e instituciones de Estados Unidos, que han tenido como consecuencia la revelación de datos personales de sus clientes (domicilios, tarjetas de crédito, productos adquiridos, etc.), los defensores de la privacidad y de los consumidores han solicitado leyes más estrictas en Estados Unidos y una mayor vigilancia de las empresas que se dedican a la compra, venta y almacenamiento de información sobre los ciudadanos.

De hecho, también podemos citar distintas sentencias relacionadas con la protección de datos en Estados Unidos. Así, por ejemplo, un tribunal de Portland (Oregón) condenó en febrero de 1999 a los miembros de una organización antiabortista al pago de una indemnización de 107 millones de dólares a médicos y clínicas relacionados con la interrupción voluntaria del embarazo, por mantener una página en Internet ("The Nuremberg Files") que la sentencia consideraba una amenaza contra los partidarios del aborto. En la página Web en cuestión se

podía acceder a las fotos de los médicos que realizan abortos y consultar su dirección y su teléfono, así como datos de los políticos y personalidades que defendían la legalidad del aborto.

Otro caso destacado es el de la cadena de lencería femenina estadounidense Victoria's Secret, que fue condenada a pagar una multa de 50.000 dólares en octubre de 2003 por no garantizar la confidencialidad de los clientes en su Website en Internet. Debido a unas medidas de seguridad deficientes, los visitantes de este Website tenían la posibilidad de consultar los pedidos de otros clientes y explorar sus gustos en materia de ropa íntima, con sólo que cambiar unos datos en la dirección URL de la página Web consultada.

A finales de marzo de 2006 se daba a conocer otra importante multa impuesta por el fiscal general de Nueva York contra la empresa estadounidense Datran Media, una empresa de mercadotecnia condenada a pagar 900.000 euros por haber empleado de forma ilegal los datos personales de seis millones de consumidores norteamericanos. Datran Media fue acusada de obtener ilegalmente direcciones de correo electrónico y otros datos personales de bases de datos de otras empresas, cuyas políticas de privacidad consistían precisamente en no compartir, vender o facilitar información personal de sus clientes "bajo ningún concepto".

Sin embargo, también podemos citar actuaciones contrarias a la protección de los datos de carácter personal. Así, por ejemplo, en septiembre de 2004 el gobernador de California, Arnold Schwarzenegger, firmó una ley que permitirá que se publique en Internet información sobre delincuentes sexuales en ese Estado, dando a los californianos un mayor acceso a los detalles sobre esas personas: nombre, fotografía, domicilio y otros detalles personales (información que sólo podía encontrarse anteriormente en lugares como las comisarías de policía de California).

Esta ley se aprobó tras un apasionado debate sobre cómo defender los derechos de los ciudadanos de peligros potenciales frente a los derechos de los individuos que salen de la cárcel tras cumplir sus condenas. La Ley Federal Megan de 1995, que recibió el nombre de una niña de 7 años que fue violada y asesinada por un vecino en una ciudad de Nueva Jersey, facultó a los Estados para crear bases de datos de delincuentes sexuales de acceso público. Todos los Estados tienen algún tipo de registro, pero varían enormemente en cuanto a la accesibilidad.

Asimismo, podemos señalar nuevos elementos de preocupación para la protección de los datos personales en Estados Unidos: la proliferación de la tecnología GPS en ese país para el seguimiento de personas; los servicios de "*phone-tracking*" o rastreo del teléfono móvil, que permiten saber en todo momento dónde se encuentra una persona (la operadora Nextel comenzó a ofrecer este servicio en 2005 por 15 dólares al mes); la recopilación de información sobre hábitos y motivos de compra por parte de empresas como Amazon, que incluso llegó a patentar en marzo de 2005 un sistema para analizar los regalos que realiza un determinado cliente, para posteriormente recordarle las fechas y ocasiones señaladas y poder sugerirle nuevos productos para la ocasión; la nueva moda de realizar búsquedas en Google sobre la vida privada, el trabajo o los gustos de otras personas; etc.

Capítulo 3

3. El marco normativo de la protección de datos personales en España

3.1. La aprobación y entrada en vigor de la LOPD.

En España el artículo 18.4 de la Constitución ya contempla que el Estado debe limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. Asimismo, en el artículo 10 de la propia Constitución se consagra el derecho a la dignidad de las personas.

La publicación de la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (en adelante LOPD), define el marco legal de la protección de los datos de carácter personal en el Estado español. Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente, de su honor e intimidad personal y familiar.

La LOPD constituye, por lo tanto, la norma fundamental que regula el tratamiento y la protección de los datos de carácter personal en España, desde su entrada en vigor el 15 de enero de 2000. Esta Ley adapta el marco normativo español a los nuevos requisitos de la Directiva Europea 46/1995, de 24 de noviembre de 1995.

Además, su entrada en vigor ha supuesto la derogación de la Ley Orgánica 5/1992, de 29 de octubre (LORTAD), ampliando el ámbito de aplicación de esta normativa a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, así como a toda modalidad de uso posterior de esos datos, es decir, ya no se limita únicamente a los ficheros que reciben un tratamiento informático o automatizado.

- Ámbito de aplicación.
- Principios de la protección de datos.
- Derechos de los ciudadanos.
- Disposiciones sectoriales.
- Movimientos internacionales de datos.
- Organismos de control: la Agencia de Protección de Datos.
- Infracciones y sanciones.

Tabla 2: *Estructura de la LOPD*

3.2. Ámbito de aplicación de la LOPD.

La LOPD se aplica a organizaciones públicas y privadas e incluso a profesionales independientes (como médicos, abogados o ingenieros) que dispongan de fuentes de datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, uso o explotación posterior. En cualquier caso el tratamiento de los datos personales (automatizado o no) debe efectuarse en el territorio español.

La Ley prevé una serie de ficheros que se encuentran excluidos, como los mantenidos por personas físicas para uso exclusivamente personal o los establecidos para la investigación de terrorismo y otras formas graves de delincuencia.

Asimismo, existen una serie de ficheros con datos de carácter personal que se rigen por sus disposiciones específicas: el censo electoral, los datos para la función estadística pública, los datos del Registro Civil y del Registro Central de Penados y Rebeldes, así como los datos procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado.

La LOPD también prevé la existencia de fuentes de acceso público: el repertorio telefónico, las listas de personas pertenecientes a grupos profesionales (en ese caso deben contener únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo), los diarios y boletines oficiales, así como los datos publicados en los medios de comunicación.

Debemos destacar que las resoluciones judiciales no pueden ser consideradas como fuente accesible al público, sin perjuicio del principio de publicidad contenido en la Ley Orgánica del Poder Judicial.

Por otra parte, la inclusión en una página Web de datos personales debe cumplir el Derecho Comunitario sobre Protección de Datos. Este tipo de tratamiento de datos no se incluye en la categoría de actividades exclusivamente personales o domésticas, según una Sentencia del Tribunal de Justicia de la Unión Europea, de noviembre de 2003, en el famoso caso "LINDQVIST".

La Sentencia del Tribunal de Justicia de la Unión Europea, que ha sentado jurisprudencia sobre esta cuestión, se refiere a una señora sueca que, durante un período en el que fue catequista en su parroquia, decidió construir desde su domicilio y con su propio ordenador personal varias páginas Web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que pudiera resultarles de ayuda. En dichas páginas Web esta señora decidió incluir datos personales sobre ella misma y dieciocho de sus compañeros de la parroquia, describiendo además en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus *hobbies* y aficiones, llegando incluso a mencionar la situación familiar y el número de teléfono.

Esta señora fue condenada finalmente a pagar una multa de aproximadamente 450 euros por haber tratado datos personales de modo automatizado sin haberlos inscrito en la Agencia Sueca de Protección de Datos y sin contar con el consentimiento expreso de los afectados, por haberlos transferido a terceros países sin autorización a través de Internet y por haber tratado incluso datos personales delicados. La afectada interpuso entonces un recurso de apelación contra esta resolución ante los tribunales suecos, quienes trasladaron la cuestión al Tribunal de Justicia de la Unión Europea, para que éste pudiera dictaminar si las supuestas infracciones eran contrarias a las disposiciones de la Directiva Europea sobre protección de los datos de carácter personal, como finalmente ocurrió en su famosa Sentencia de noviembre de 2003.

3.3. *Responsable del fichero.*

La LOPD define el responsable del fichero o tratamiento como la persona física o jurídica, de naturaleza pública o privada, que decide sobre la finalidad, contenido y uso del tratamiento de los datos.

El responsable de una serie de ficheros de datos de carácter personal tiene que asumir las siguientes obligaciones:

1. Elaborar un documento de seguridad, que deberá mantenerse actualizado y adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.
2. Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad y las consecuencias de su incumplimiento.
3. Implantar un mecanismo de identificación de usuarios.
4. Mantener una relación de los usuarios del sistema con los derechos de acceso a los datos y aplicaciones.
5. Establecer mecanismos para evitar que los usuarios accedan a recursos con derechos distintos de los autorizados.
6. Verificar los procedimientos de copia y de recuperación de datos.
7. Autorizar por escrito la ejecución de procedimientos de recuperación de datos.
8. Autorizar expresamente el tratamiento fuera de los locales de la organización.
9. Autorizar la salida de soportes informáticos fuera de los locales de la organización.
10. Designar al responsable o responsables de seguridad, si fuera necesario.
11. Adoptar las medidas correctoras de las deficiencias detectadas en las auditorías de seguridad.

Tabla 3: *Obligaciones del responsable de los ficheros*

Suele ser bastante habitual, por otra parte, que la empresa u organismo responsable del fichero decida encargar su tratamiento a un tercero. Tal es el caso, por ejemplo, de la contratación a una gestoría de la confección de las nóminas del personal, de la contratación de un proceso de selección de personal a una empresa especializada, de la contratación del servicio de atención telefónica a un "*call-center*", etc.

Por lo tanto, de acuerdo con lo establecido por la LOPD, el encargado del tratamiento es aquella persona física o jurídica que realice algún trabajo sobre los datos personales por cuenta del responsable del fichero. Tiene responsabilidad conjunta con el responsable del fichero sobre el establecimiento de las medidas de seguridad.

Asimismo, el encargado del tratamiento tiene la obligación de indemnizar por los daños que los interesados pudieran sufrir como consecuencia del incumplimiento por su parte de las obligaciones de la LOPD.

Conviene tener en cuenta, no obstante, que de acuerdo con el artículo 12 de la LOPD, la realización de un tratamiento por cuenta de un tercero deberá estar regulada en un contrato en el que se establezca expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del fichero, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En este contrato se estipularán, asimismo, las medidas de seguridad de carácter técnico y organizativo que el encargado del tratamiento estará obligado a implementar.

De este modo, la LOPD impide una posible subcontratación del tratamiento de los datos, debiendo figurar siempre el responsable del fichero como parte en la relación jurídica con cada uno de los encargados del tratamiento.

3.4. Principios de la protección de los datos.

El marco normativo de la LOPD establece una serie de principios relativos al tratamiento y protección de los datos de carácter personal:

3.4.1. Principio fundamental de "Habeas Data".

El principio de "*habeas data* " (que podríamos traducir por la expresión 'tenga yo los datos') fue fijado en España por una sentencia del Tribunal Supremo del 30 de noviembre de 2000, en la que se afirma que los datos personales son del ciudadano, no de la organización que decide crear un fichero en el que se incluyan dichos datos.

Asimismo, esta sentencia reconoce el derecho fundamental a la Protección de Datos Personales, considerando que éste viene determinado por la "facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y por otro lado, el poder oponerse a esa posesión y usos".

3.4.2. Calidad de los datos.

Los datos personales que vayan a ser tratados por una determinada empresa o institución deben ser adecuados, pertinentes y no excesivos, en relación con el ámbito y finalidades legítimas para las que se hayan obtenido.

Así, por ejemplo, una empresa podrá utilizar datos identificativos, de filiación, académicos, profesionales y bancarios de sus empleados para confeccionar las nóminas o registrar su situación profesional en la organización, pero se podría considerar que se estaría excediendo más allá de la finalidad prevista (incumpliendo, por tanto, el principio de "calidad de los datos") si también se recabasen datos sobre sus aficiones y *hobbies*, tal y como ha expresado la Agencia Española de Protección de Datos en alguno de sus informes jurídicos.

Los datos de carácter personal serán conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la empresa y el interesado. Además, los datos deben ser exactos y estar puestos al día para garantizar su veracidad y tendrán que ser cancelados en cuanto hayan dejado de ser necesarios para la organización.

3.4.3. Seguridad de los datos.

La LOPD establece en su artículo 9 que el responsable del fichero y, en su caso, el encargado del tratamiento, deberán adoptar las medidas necesarias de índole técnica y organizativa para garantizar la seguridad de los datos de carácter personal y que puedan evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

3.4.4. Deber de secreto.

Las personas y empresas que intervengan en cualquier fase del tratamiento de datos de carácter personal deben comprometerse a guardar el debido secreto profesional respecto de los mismos, incluso después de haber finalizado la relación que les unía con la entidad poseedora de los datos personales.

3.4.5. Información en la recogida de datos.

El responsable del fichero debe informar a los interesados antes de proceder al tratamiento de sus datos de carácter personal, indicando el fichero (o ficheros) en que se van a incorporar sus datos, la finalidad del tratamiento y los posibles destinatarios de estos datos.

Asimismo, en todos los formularios en papel o en las páginas Web utilizadas para recabar datos de carácter personal, es necesario incluir cláusulas informativas acerca de la naturaleza y la finalidad del tratamiento. En otro caso, la Ley requiere que en un plazo de tres meses se informe al interesado del tratamiento al que están siendo sometidos sus datos personales por parte de la empresa, salvo cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le deberá informar del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

Por otra parte, en caso de obtener datos mediante cámaras de videovigilancia (por motivos de seguridad), será necesario informar a los ciudadanos de que se están registrando sus imágenes en un sistema de seguridad.

En lo que se refiere a la privacidad de los usuarios que visitan un determinado sitio Web, la empresa o institución responsable debe dejar clara cuál es su Política de Privacidad, informando sobre la utilización de "*cookies*" u otros mecanismos que permitan realizar un seguimiento de las visitas al Website, tal y como establece en España la Ley General de Telecomunicaciones (Ley 32/2003, de 3 de noviembre): se debe informar a los usuarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

3.4.6. Consentimiento del afectado para el tratamiento.

El artículo 3.h de la LOPD define el consentimiento del interesado como "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".

Como norma de partida, la LOPD establece que el tratamiento de los datos de carácter personal requiere del consentimiento inequívoco del afectado, siendo necesario que este consentimiento figure además por escrito cuando se trate de datos especialmente protegidos.

No obstante, se han previsto una serie de excepciones a esta norma, en los casos siguientes:

- Datos personales obtenidos de fuentes accesibles al público.
- Datos necesarios para el ejercicio de funciones de la Administración, como podría ser el caso de la prestación de los distintos servicios de un ayuntamiento o la recaudación de los tributos locales.
- Datos de personas vinculadas mediante una relación negocial, laboral, administrativa o contractual, siempre y cuando estos datos sean necesarios para mantener dicha relación o para la celebración del contrato que vincula a ambas partes.
- Cuando los datos personales recabados afecten a la Defensa Nacional, la seguridad pública o la persecución de infracciones penales.

Por supuesto, se prohíbe la recogida por medios fraudulentos, desleales o ilícitos, siendo considerada esta práctica como una infracción muy grave de la LOPD.

3.4.7. Comunicación o cesión de datos a terceros.

La comunicación o cesión de datos de carácter personal sólo es posible si existe un consentimiento previo del afectado, tras haber sido informado sobre la finalidad de la comunicación o las actividades del cesionario, siempre y cuando además la cesión sea necesaria para el cumplimiento de fines directamente relacionados con funciones legítimas del cedente y cesionario.

No obstante, la LOPD ha previsto una serie de excepciones a la norma anterior, de tal forma que la cesión podrá ser realizada sin el consentimiento previo del afectado en las siguientes circunstancias:

- Cuando la cesión haya sido autorizada por otra ley, como podría ser el caso de la cesión a la Agencia Estatal para la Administración Tributaria de datos económicos y fiscales de empleados, proveedores y clientes de una empresa, en virtud de lo dispuesto por la Ley General Tributaria.
- Cuando los datos cedidos hayan sido obtenidos de fuentes accesibles al público.
- Cuando la cesión de datos sea necesaria para el desarrollo, cumplimiento y control de una relación jurídica libre y legítimamente aceptada por ambas partes.
- Otros casos previstos: cesiones entre Administraciones Públicas con fines históricos, estadísticos o científicos; cesiones en las que el destinatario sea el Defensor del pueblo, el Ministerio fiscal o los Tribunales; cuando por razones de urgencia sea preciso ceder datos relativos a la salud del interesado.

Por lo tanto, debemos tener muy presente que las cesiones de datos entre empresas de un mismo grupo requieren del consentimiento previo e inequívoco de los afectados, siendo necesario identificar explícitamente las finalidades a las que se destinarán los datos cedidos.

La LOPD en su artículo 11.5 también establece la responsabilidad para la empresa adquirente de los datos como resultado de una cesión, la cual deberá cumplir con todos los requisitos de esta Ley.

Asimismo, conviene insistir en la distinción entre una cesión de datos a un tercero y un tratamiento de datos encargado a un tercero y realizado por cuenta del responsable del fichero. En este segundo caso, no se considera que se esté produciendo una cesión, por lo que no es necesario recabar el consentimiento de los afectados.

Pero para que se considere un tratamiento encargado a un tercero y no una cesión, la LOPD establece que es necesario formalizar mediante un contrato por escrito u otra forma que deje constancia del contenido del tratamiento, reflejando expresamente que el encargado tratará los datos según las instrucciones del responsable del fichero, que el encargado no podrá comunicar los datos a terceros ni tan siquiera para su conservación y que

deberá implantar una serie de medidas de carácter técnico y organizativo para garantizar su seguridad. Una vez concluida la prestación del servicio, los datos tendrán que ser devueltos al responsable del fichero o bien destruidos de forma segura.

Por otra parte, en estos últimos años, se ha planteado una cierta polémica en España debido a las cesiones de datos de clientes realizadas por operadores de telecomunicaciones a distintas filiales suyas (o incluso a otras empresas), tras haber informado por escrito a los afectados solicitando su consentimiento tácito o implícito. Así, por ejemplo, el envío de cartas no certificadas por parte de grandes empresas (como los operadores de telecomunicaciones) solicitando el consentimiento de sus clientes para ceder datos a alguna de sus filiales o sociedades integradas en su grupo ha sido considerada como una práctica conforme con lo previsto por la LOPD, siempre y cuando en dicha carta se informe con claridad de las condiciones de la cesión y se dé la opción de que el interesado pueda expresar su oposición a la cesión.

Conviene destacar que, si bien la Agencia de Protección de Datos ha admitido la posibilidad de obtener un consentimiento tácito ("si usted no manifiesta su rechazo a la medida en un plazo de 30 días, entendemos que consiente la cesión de sus datos"), las empresas deben precisar de forma explícita cuál es la finalidad del tratamiento de esos datos.

La Agencia de Protección de Datos sostiene que "no serán válidas expresiones genéricas" por parte de las empresas a la hora de solicitar el consentimiento de sus clientes para la utilización de sus datos. Asimismo, la carga de la prueba sobre la recepción de la misiva en la que se solicita el consentimiento al interesado recae sobre la empresa, de modo que si el interesado niega haber recibido la comunicación, será la empresa que utiliza los datos la que deberá acreditarlo.

De acuerdo con la postura mantenida por la Agencia de Protección de Datos, para denegar el consentimiento las personas afectadas no tendrán por qué realizar el procedimiento exclusivamente por escrito, sino que podrán recurrir a otras fórmulas como la comunicación a través del servicio de atención al cliente o directamente en alguna de las oficinas de la empresa en cuestión.

3.4.8. Transferencias de datos personales a terceros países.

La LOPD establece que no se podrán efectuar transferencias de datos personales (ya sean éstas temporales o definitivas) a países sin un nivel de protección equiparable al de España, salvo que se disponga de una autorización previa del director de la Agencia Española de Protección de Datos o que el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

Se consideran países que proporcionan un nivel de protección adecuado de los datos de carácter personal todos los estados miembros de la Unión Europea o un Estado respecto del cual la Comisión de la Unión Europea haya declarado que garantiza un nivel de protección adecuado. Hasta la fecha se encuentran incluidos entre estos últimos Suiza, Hungría, Argentina y Canadá, así como las entidades estadounidenses que se han adherido a los "principios de Puerto Seguro".

3.4.9. Datos especialmente protegidos.

Se consideran "datos especialmente protegidos" aquellos datos de carácter personal referentes a la ideología, salud, vida sexual, origen racial, religión o creencias. Para estos datos la LOPD contempla un nivel mayor de protección.

En España el artículo 16 de la Constitución ya establece que nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Por este motivo, quedan totalmente prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, origen racial o étnico, religión, creencias o vida sexual.

Los datos sobre el origen racial, salud y vida sexual de las personas sólo podrán ser tratados con el consentimiento expreso del afectado o bien cuando así lo disponga una ley. Se contempla la excepción en los casos de prevención o diagnóstico médico, prestación de asistencia sanitaria o tratamientos médicos, así como cuando sea necesario para salvaguardar el interés vital del afectado.

Los datos personales que puedan revelar la ideología, afiliación sindical, religión y creencias sólo podrán ser tratados cuando existe el consentimiento expreso y por escrito del afectado. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros. La cesión de dichos datos requerirá siempre el consentimiento previo del afectado.

Por otra parte, los datos relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes, de conformidad con sus normas reguladoras.

3.4.10. Datos relativos a la salud de las personas.

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

Sobre esta cuestión conviene tener en cuenta la Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que entró en vigor el 15 de mayo de 2003, en la que se establecen determinadas obligaciones que deben cumplir los centros de salud y las Administraciones sanitarias:

- El archivo de las historias clínicas de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.

- El establecimiento de mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura.

- La adopción de medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental.

- La implantación de un sistema de compatibilidad que, teniendo en cuenta la evolución y disponibilidad de los recursos técnicos, así como la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente.

3.5. Derechos de los ciudadanos.

La LOPD reconoce determinados derechos de los ciudadanos en relación con la información, el acceso y el nivel de control sobre el tratamiento de sus datos de carácter personal:

- **Derecho de información en la recogida de los datos**.

Los interesados a los que se soliciten datos personales deben ser previamente informados de modo expreso, preciso e inequívoco, de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

- **Derecho de consulta al Registro General de Protección de Datos**.

Se trata, en este caso, del derecho a conocer del Registro la existencia de tratamientos de datos, sus finalidades y la identidad del responsable del tratamiento. De hecho, cualquier ciudadano puede acceder gratuitamente a través de la página Web de la Agencia Española de Protección de Datos para consultar los ficheros declarados por cualquier empresa u organismo público.

Figura 5: Consulta en el Registro General de Protección de Datos

En el Registro General de Protección de Datos se pueden obtener los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

- **Derecho de acceso a sus datos de carácter personal**.

De acuerdo con el artículo 15 de la LOPD, todo ciudadano tiene derecho a solicitar y obtener gratuitamente información acerca de qué datos relativos a su persona se encuentran sometidos a tratamiento, el origen de dichos datos y las posibles cesiones de éstos. La LOPD contempla además un plazo de un mes para hacerlo efectivo, es decir, la organización que reciba una petición en este sentido formulada por un ciudadano deberá resolverla en un plazo de un mes. Se ha previsto un período de 12 meses para que el ciudadano en cuestión pueda volver a ejercer este derecho ante la misma organización.

- **Derecho de rectificación y cancelación**.

La LOPD considera que el ejercicio de este derecho es personalísimo y la empresa u organismo que reciba la petición dispondrá de un plazo de 10 días naturales para hacerlo efectivo y dar respuesta expresa al interesado, tal y como se establece en el artículo 16 de la LOPD.

Hay que tener en cuenta que en muchos casos la cancelación dará lugar al bloqueo de los datos pero no a su eliminación inmediata, de tal forma que éstos podrán conservarse en las bases de datos de la organización, estando disponibles para la Administración, jueces y tribunales durante el período de prescripción de las posibles responsabilidades. Los datos deberán ser destruidos una vez hayan prescrito estas responsabilidades.

Por otra parte, en el caso de que se hayan cedido los datos a terceros, el responsable del fichero se encargará de comunicar la petición de rectificación o cancelación a todas aquellas empresas e instituciones a las que haya comunicado los datos, para que puedan proceder de igual modo.

- **Derecho de oposición**.

Todo ciudadano podrá oponerse al tratamiento de sus datos, aún cuando se trate de aquellos datos para los que no sea necesario su consentimiento previo (datos procedentes de fuentes accesibles al público). Ante esta petición planteada por un ciudadano, el responsable del fichero está obligado a excluir del tratamiento los datos relativos al afectado (situación típica de un ciudadano que manifiesta su deseo de no seguir recibiendo información publicitaria en su domicilio).

- **Derecho a indemnización**.

De acuerdo con lo dispuesto en el artículo 19 de la LOPD, si como consecuencia del incumplimiento de alguno de los preceptos de esta Ley Orgánica se pudieran producir daños al afectado, a sus bienes o a sus derechos se podría generar un derecho de indemnización, bien de acuerdo con el procedimiento establecido de responsabilidad de las Administraciones Públicas, en el caso de los ficheros de titularidad pública, o bien ante los Tribunales ordinarios para los ficheros de titularidad privada.

Por último, para completar este apartado es necesario destacar que la Agencia Española de Protección de Datos puede ejercer la tutela de derechos de los interesados.

3.6. *Agencia Española de Protección de Datos.*

La Agencia Española de Protección de Datos es el organismo público encargado de velar por el cumplimiento de la legislación sobre protección de datos.

Figura 6

Sus competencias básicas son las que se enumeran a continuación:

- Velar por el cumplimiento de la LOPD y de sus disposiciones reglamentarias.
- Dictar instrucciones para adecuar los tratamientos y seguridad de los ficheros (capacidad normativa).
- Velar por la publicidad de la existencia de los ficheros de datos.
- Ejercer la potestad inspectora y sancionadora.

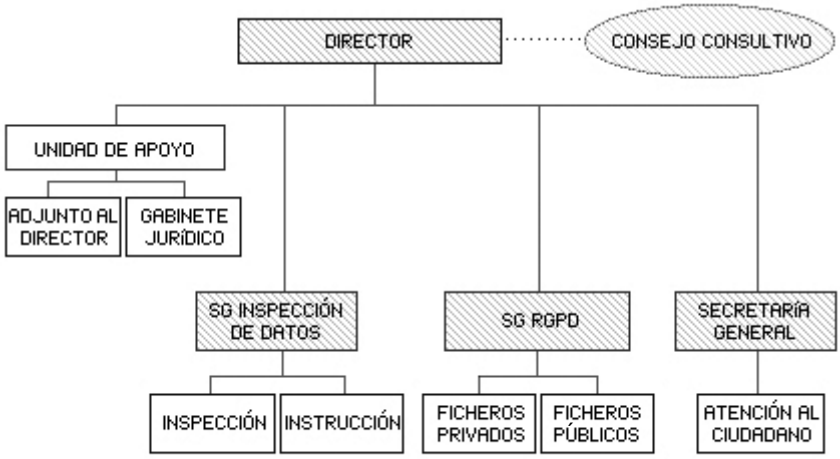


Figura 7: *Organigrama de la Agencia Española de Protección de Datos*

Se trata de un organismo de carácter autónomo, que no está sometido ni depende jerárquicamente de ninguna otra institución. De hecho, la Agencia de Protección de Datos posee un Estatuto propio, aprobado por el Gobierno. El Director de la Agencia es un Alto Cargo de la Administración, nombrado por cuatro años, que no está sujeto a instrucción alguna en el desempeño de sus funciones.

La Agencia de Protección de Datos también se encarga del mantenimiento del Registro General de Protección de Datos (RGPD), en el que se deben inscribir tanto los ficheros de titularidad privada como de titularidad pública, así como los distintos códigos tipo y las autorizaciones de transferencias internacionales de datos de carácter personal con destino a países que no presten un nivel de protección equiparable al de la Unión Europea.

En la siguiente tabla se presenta la evolución del número de ficheros inscritos en el Registro General de Protección de Datos en estos últimos años:

	31/12/94	31/12/95	31/12/96	31/12/97	31/12/98	31/12/99	31/12/00	31/12/01	31/12/02	31/12/03	31/12/04
Titularidad Pública	20.198	24.923	26.541	27.969	28.890	30.431	31.155	31.805	35.894	43.974	48.038
Titularidad Privada	192.097	199.933	201.054	201.835	203.138	204.737	218.054	240.070	292.755	361.675	457.490
Total	212.295	224.856	227.595	229.804	232.028	235.168	249.209	271.875	328.649	405.649	505.528

Tabla 4: Ficheros inscritos en el Registro General de Protección de Datos

Conviene destacar la ampliación de las competencias establecida por la Ley General de Telecomunicaciones (Ley 32/2003, de 3 de noviembre). Esta Ley atribuye a la Agencia la tutela de los derechos y garantías de abonados (entendiendo como tales a las personas físicas o jurídicas con contrato con un operador de telecomunicaciones) y usuarios (quienes utilizan los servicios sin haberlos contratado) en el ámbito de las comunicaciones electrónicas.

Asimismo, desde el 20 de marzo de 2004 corresponde a la Agencia de Protección de Datos la imposición de sanciones en el caso de infracciones por el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico (*spam*). En España la Ley de Servicios de la Sociedad de la Información (LSSI, Ley 34/2002, de 11 de julio) prohíbe expresamente el envío de comunicaciones publicitarias por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

3.7. Órganos de control autonómicos.

La propia Ley Orgánica de Protección de Datos ha previsto en su artículo 41 la creación de órganos de control autonómicos. Estas Agencias Autonómicas sólo podrán tener competencias sobre las Administraciones Públicas, entes locales, Universidades públicas y corporaciones de ámbito público dentro de las distintas Comunidades Autónomas.

En la actualidad en España existen tres Agencias Autonómicas de Protección de Datos: la Agencia Madrileña, la Agencia Catalana y la Agencia Vasca.

Es necesario destacar que, a diferencia de la Agencia Española, las Agencias de Protección de Datos Autonómicas no cuentan con otros ingresos para financiar su actividad que la dotación anual presupuestaria con cargo a los Presupuestos Generales de la Comunidad Autonómica en la que actúan, ya que todos sus servicios se ofrecen a título gratuito, con la excepción de la venta de algunas publicaciones a través de sus páginas Web. Sólo la Agencia Española de Protección de Datos puede imponer sanciones económicas, ya que es la única con competencias para inspeccionar a empresas e instituciones responsables de ficheros de titularidad privada.

Entre sus competencias podríamos destacar las siguientes:

- Vigilar el cumplimiento de la legislación sobre protección de datos de carácter personal en la Administración Pública de esa Comunidad Autónoma, así como en las Administraciones Locales, Universidades públicas y otras Corporaciones de Derecho Público de esa Comunidad Autónoma.
- Mantener un Registro de Ficheros de Datos Personales de la Comunidad Autónoma, relativo a ficheros de titularidad pública.
- Ejercer labores de inspección y control sobre los ficheros con datos de carácter personal sujetos a su ámbito competencial, interviniendo de oficio o a instancia del ciudadano cuando los tratamientos de estos ficheros no se ajusten a la normativa vigente sobre Protección de Datos.
- Realizar actividades de formación y sensibilización sobre Protección de Datos.
- Atender a las consultas realizadas por los ciudadanos a través de distintos medios: en persona, por teléfono, por fax, carta, correo electrónico, etc.

La Agencia de Protección de Datos de la Comunidad de Madrid (www.apdcm.es) fue creada en 1995, siendo la decana de las Agencias Autonómicas en el Estado Español. Su marco de actuación se ha establecido mediante la Ley de Protección de Datos de la Comunidad de Madrid (Ley 8/2001 de 13 de julio) y por el Decreto 40/2004, de 18 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid.

Por su parte, la Agencia de Protección de Datos de la Comunidad de Cataluña (www.apdcat.net) fue creada en 2003. Su marco de actuación se ha establecido mediante la Ley 5/2002 de 19 de abril, del Parlamento de Cataluña y el Decreto 48/2003 de 20 de febrero.

La Agencia de Protección de Datos del País Vasco (www.avpd.euskadi.net) fue creada en 2004. Su marco de actuación se ha establecido mediante la Ley 2/2004 de Protección de Datos del País Vasco.

3.8. Inscripción de ficheros con datos de carácter personal.

Todo titular de un fichero con datos de carácter personal debe notificar su existencia a la Agencia de Protección de Datos, antes de la puesta en marcha de la base de datos o aplicación informática donde se vayan a tratar los datos de dicho fichero. En la declaración de inscripción es necesario especificar la estructura (tipo de datos que se van a recabar de los interesados), la finalidad del tratamiento de los datos, el nivel de medidas de seguridad que se van a adoptar para garantizar su seguridad, así como las posibles cesiones y/o tratamientos encargados a terceros.

En la siguiente tabla se recogen los apartados que forman parte del modelo oficial para la inscripción de los ficheros de titularidad pública:

1. Responsable del fichero.
2. Servicio o Unidad concreto ante el que puedan ejercitarse los derechos de oposición, acceso, rectificación y cancelación.
3. Disposición general de creación, modificación o supresión del fichero.
4. Nombre y descripción del fichero o tratamiento de datos.
5. Encargado del tratamiento.
6. Nivel adoptado para las Medidas de Seguridad (Básico, Medio o Alto).
7. Estructura básica y descripción de los tipos de datos de carácter personal incluidos en el fichero.
8. Declaración de la finalidad del fichero y de los usos previstos.
9. Personas o colectivos sobre los que se van a obtener datos personales.
10. Procedencia y procedimiento de recogida de los datos.
11. Cesiones o comunicaciones previstas de los datos.
12. Transferencias internacionales de datos.

Tabla 5: Inscripción de ficheros de titularidad privada.

Cada notificación de inscripción se corresponderá con el tratamiento de un fichero con datos de carácter personal. Se trata de un procedimiento totalmente gratuito, que se puede llevar a cabo mediante un formulario oficial o bien a través de una aplicación informática que se puede descargar de la propia página Web de la Agencia de Protección de Datos y que permite realizar la inscripción a través de Internet.

Posteriormente será necesario comunicar a la Agencia las modificaciones realizadas en estos ficheros o su posible cancelación.

Para los ficheros preexistentes, el plazo para su inscripción en el Registro General de Protección de Datos terminó el 15 de enero de 2003, tres años después de la entrada en vigor de la LOPD. Sin embargo, para los ficheros y tratamientos no automatizados se concedió un plazo de 12 años que expirará el 24 de octubre de 2007.

3.9. Implantación de las medidas de seguridad sobre los ficheros.

El Reglamento de Medidas de Seguridad fue aprobado mediante el Real Decreto 994/1999, de 11 de junio de 1999, entrando en vigor el 26 de junio de 1999. Se trata, por tanto, de un Reglamento previo a la aprobación de la propia LOPD, que determina las medidas de índole técnica y organizativa que se deben adoptar para garantizar la integridad y seguridad de ficheros automatizados, centros de tratamiento, locales, equipos, sistemas, programas, así como de las personas que intervengan en el tratamiento automatizado de los datos.

De hecho, el artículo 9.2 de la LOPD establece que no se podrán registrar datos de carácter personal en ficheros que no reúnan unas condiciones adecuadas con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

También resulta aplicable este Reglamento a los ficheros en soporte no automatizado que se hubieran creado con posterioridad a la entrada en vigor de la LOPD, el 15 de enero de 2000. En este caso, deberán implantarse las medidas de seguridad que, pese a estar previstas para tratamientos automatizados, por su naturaleza sean también aplicables a ficheros no automatizados. Sin embargo, la Agencia de Protección de Datos no ha establecido cuáles son estas medidas ni cómo tendrían que ser implantadas. Los ficheros en soportes no automatizados que ya existieran con anterioridad a la entrada en vigor de la LOPD dispondrán del período de adaptación establecido en la Disposición Adicional Primera de esta Ley, que finaliza en octubre de 2007.

En el citado Reglamento se establecen tres "**Niveles de Seguridad**" para los datos de carácter personal:

- **Nivel Básico**: de aplicación a todos los ficheros de datos de carácter personal.
- **Nivel Medio**: de aplicación a los ficheros que contengan datos relativos a la comisión de infracciones, Hacienda Pública, servicios financieros. Asimismo, se consideran dentro de este nivel aquellos ficheros que contengan un conjunto de datos de carácter personal que permitan obtener una evaluación de la personalidad del individuo.

- **Nivel Alto**: de aplicación a los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los recabados para fines policiales.

Independientemente del nivel de los datos tratados, el Reglamento de Medidas de Seguridad establece que las medidas de seguridad para el tratamiento de datos a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente a los accesos en modo local. Asimismo, cuando se vaya a realizar un trabajo con los ficheros fuera de los locales en los que se haya declarado que se realiza su tratamiento, Este trabajo deberá ser autorizado y llevarse a cabo garantizando los mismos niveles de seguridad. Del mismo modo, cuando se trabaje con ficheros temporales, éstos deberán ser borrados una vez concluida su utilidad y durante su existencia deberán tener las mismas medidas de seguridad que los originales de los que han sido extraídos.

Las medidas de seguridad mínimas que se han de adoptar en el Nivel Básico, y que también son de aplicación en los niveles Medio y Alto, han de contemplar los siguientes aspectos:

- Elaboración de un Documento de Seguridad que incluya la siguiente información:
  - Ámbito de aplicación del documento con una especificación detallada de los recursos protegidos.
  - Medidas, normas y procedimientos adoptados para garantizar el nivel de seguridad.
  - Funciones y obligaciones del personal.
  - Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
  - Procedimiento de notificación y gestión de incidencias.
  - Procedimiento de realización de copias de seguridad.
  - El documento deberá mantenerse en todo momento actualizado y tendrá que ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Asimismo, este documento debe ser aprobado por la Dirección, estar implantado y ser divulgado entre los empleados con acceso a los datos.
- Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal estarán claramente definidas y documentadas, manteniendo en todo momento una relación actualizada de usuarios que tienen acceso a estos datos.
- Se ha de establecer un sistema de identificación y autenticación de los usuarios con acceso a los datos de carácter personal.
- Se ha de establecer un sistema de control de acceso a los datos de carácter personal, con los mecanismos necesarios para impedir que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

- Los usuarios deben tener acceso únicamente a los datos que necesitan para el desempeño de sus funciones.
- Los mecanismos deben evitar el acceso a datos no autorizados.
- Debe existir una relación de usuarios con los accesos autorizados.
- Únicamente personal autorizado puede conceder y modificar los derechos de acceso a los ficheros.

- Se deberá llevar a cabo una correcta gestión de los soportes informáticos que contengan datos de carácter personal:
  - Identificación e inventariado de los soportes, que deberán almacenarse en un lugar con acceso restringido al personal autorizado.
  - La salida de soportes informáticos que contengan datos de carácter personal fuera de los locales en los que esté ubicado el fichero sólo podrá ser autorizada por el responsable del fichero.
- Los procedimientos establecidos para la realización de copias de seguridad de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Para ello se deberán realizar copias de seguridad al menos una vez por semana, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
- Gestión de incidencias: el procedimiento de notificación y gestión de incidencias contendrá necesariamente 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 y los efectos que se hubieran derivado de la misma.

En lo que se refiere a las medidas de seguridad adicionales que se han de adoptar en el Nivel Medio, debemos tener en cuenta los siguientes aspectos:

- El Documento de Seguridad deberá contener, además de lo dispuesto en las medidas del Nivel Básico, la siguiente información:
  - Identificación del responsable o responsables de la seguridad.
  - Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.
  - Procedimientos para el tratamiento de soportes desechados o reutilizados.
  - Procedimientos para el control de los registros de entradas y salidas de soportes.
  - Plan auditor.

- Existencia de un responsable de seguridad: el responsable del fichero designará uno o varios responsables de seguridad, personas encargadas de coordinar y supervisar la implantación y el nivel de cumplimiento de las medidas definidas en el documento de seguridad.

- Identificación y autentificación de los usuarios: será necesario establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información de la empresa. Dicho mecanismo de identificación limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

- Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

- Gestión de soportes: será necesario establecer un sistema de registro de entradas y salidas de soportes informáticos que permita conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega o recepción que deberá estar debidamente autorizada.

    - Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en el mismo.

    - Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

- En el registro de incidencias se anotarán todos los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso y cuáles han sido los datos restaurados.

- Copias de seguridad: será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

- 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 tipo de fichero tratado.

- Auditoría de la seguridad: los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento de las medidas, procedimientos e instrucciones vigentes en materia de seguridad de datos. Esta auditoría tendrá lugar al menos una vez cada dos años y el informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

Por último, las medidas de seguridad adicionales que se han de adoptar en el Nivel Alto deben tener en cuenta los siguientes aspectos:

- Encriptación de los ficheros con datos de carácter personal:
    - Los datos de los soportes que vayan a ser distribuidos deberán estar convenientemente encriptados, para garantizar que dicha información no sea inteligible ni manipulada durante su transporte.
    - La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará encriptando dichos datos, para garantizar que la información no sea inteligible ni manipulada por terceros.
- Establecimiento de un registro de control de accesos al fichero: se deberá registrar cada intento de acceso, especificando 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. Asimismo, en caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. Este registro de control de los accesos deberá conservarse durante un período mínimo de dos años.
- Copias de seguridad: estas copias deberán conservarse en un lugar diferente de aquél en que se encuentren los equipos informáticos que contienen los datos de carácter personal.

Se establecieron los siguientes plazos para la implantación de las medidas de seguridad descritas en el Reglamento:

- Nivel Básico: 26 de marzo de 2000.
- Nivel Medio: 26 de junio de 2000.
- Nivel Alto: 26 de junio de 2001. No obstante, se concedió una prórroga hasta el 26 de junio de 2002 para los casos en que estuviera justificado debido a la obsolescencia tecnológica del sistema de información de la organización afectada.

Una vez documentadas todas estas medidas de seguridad es necesario llevarlas a la práctica, tal y como señala una Sentencia de la Audiencia Nacional del 7 de febrero de 2003: "no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Así, de nada sirve que se aprueben unas instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales si luego no se exige a los empleados de la entidad la observancia de aquellas instrucciones".

3.10. *Infracciones y sanciones.*

La LOPD establece la existencia de tres tipos de infracciones: leves, graves y muy graves.

Así, como infracciones leves podemos citar las siguientes:

- No atender una solicitud del interesado de rectificación o cancelación de los datos personales.
- No solicitar la inscripción del tratamiento de un fichero con datos de carácter personal en el Registro General de Protección de Datos.
- Proceder a la recogida de datos de carácter personal sin proporcionar información a los afectados.
- Incumplir el deber de secreto.

Entre las infracciones graves se encuentran las que se enumeran a continuación:

- Proceder a la creación de ficheros de titularidad privada con finalidades distintas de las que constituyen el objeto legítimo.
- Proceder a la recogida de datos de carácter personal sin el consentimiento expreso de las personas afectadas.
- Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la LOPD.
- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que procedan.
- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad.

Por último, merecen la consideración de infracciones muy graves actuaciones como las que se indican a continuación:

- La recogida de datos en forma engañosa y fraudulenta.
- La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
- Recabar y tratar los datos de carácter personal especialmente protegidos sin cumplir los requisitos exigidos por la LOPD.
- No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

- La transferencia temporal o definitiva de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin la correspondiente autorización del Director de la Agencia de Protección de Datos.

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

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

Las infracciones leves prescriben en el plazo de un año, mientras que las infracciones graves lo hacen al cabo de dos años y las muy graves en un plazo de tres años.

Conviene destacar que la LOPD define, con diferencia, el régimen sancionador más severo de toda la Unión Europea en materia de protección de datos de carácter personal. No obstante, en otros países como Italia o Portugal también se han establecido penas de prisión para los transgresores de la legislación en materia de protección de datos, mientras que en España sólo se ha contemplado la vía de la sanción administrativa.

Así, en España para las infracciones leves se prevén multas de 100.000 a 10.000.000 de pesetas (601 € a 60.101 €). Para las infracciones graves las multas pueden situarse entre los 10.000.000 y los 50.000.000 de pesetas (60.101 € a 300.506 €). Por último, en el caso de las infracciones muy graves, las multas se aplicarán en el intervalo de 50.000.000 a 100.000.000 de pesetas (300.506 € a 601.012 €), contemplándose además la potestad de inmovilización de los ficheros por parte de la propia Agencia de Protección de Datos.

La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, el volumen de los tratamientos efectuados, los beneficios obtenidos por la organización responsable, el grado de intencionalidad, la reincidencia, los daños y perjuicios causados a las personas interesadas, etc.

El procedimiento sancionador se iniciará siempre de oficio mediante acuerdo del Director de la Agencia de Protección de Datos, bien por denuncia de un afectado o afectados o por propia iniciativa.

No obstante, si las infracciones se cometen en el tratamiento de ficheros de titularidad pública no se impondrá ninguna sanción económica, tal y como establece el artículo 46 de la LOPD. En estos casos, el Director de la Agencia de Protección de Datos podrá proponer la adopción de medidas disciplinarias, de acuerdo con lo establecido por el Régimen Disciplinario de las Administraciones Públicas.

3.11. Evolución de la normativa sobre Protección de Datos.

3.11.1. Normativa básica.

En este apartado se recoge la evolución de la normativa en materia de Protección de Datos de Carácter Personal:

- Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales.
- **Ley Orgánica 5/1992**, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (**LORTAD**).
- Real Decreto 428/1993, de 26 de junio, Estatuto de la Agencia de Protección de Datos.
- Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992 de 29 de octubre.
- Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito.
- Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.
- **Directiva 95/46/CE**, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (plazo de transposición de 3 años).
- Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos.
- Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos para controlar el acceso a los edificios.
- Instrucción 2/1996, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.
- **Directiva 97/66/CE**, de 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (plazo de transposición hasta el 24 de octubre de 1998).

- Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
- **Real Decreto 994/1999**, del 11 de junio de 1999, por el que se aprueba el **Reglamento de Medidas de Seguridad** de los ficheros automatizados que contengan datos de carácter personal.
- **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal (**LOPD**).
- Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implementar las Medidas de Seguridad de los Ficheros Automatizados previstas por el Reglamento.
- Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas que rigen los movimientos internacionales de datos.
- **Ley 34/2002**, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE).
- **Directiva 2002/58/CE**, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en las comunicaciones electrónicas (recogida por la nueva Ley General de Telecomunicaciones, Ley 32/2003, de 3 de noviembre).
- **Ley 32/2003**, de 3 de noviembre, General de Telecomunicaciones (LGT).
- Reglamento (CE) Número 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros (DOCE del 29 de diciembre de 2004).
- Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos, sobre publicación de sus Resoluciones (BOE del 5 de enero de 2005).

Durante el año 2005 la Agencia Española de Protección de Datos ha estado trabajando en la elaboración de un Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, cuya entrada en vigor se prevé para mediados de 2006.

En este nuevo Reglamento se establecerán cuáles son las medidas de seguridad aplicables a los ficheros de carácter personal no automatizados (los que todavía se encuentran en soporte papel, por ejemplo). Asimismo, en el borrador de este Reglamento se ha previsto un cierto "endurecimiento" de las medidas de seguridad aplicables a los ficheros considerados como de nivel medio, ya que se les tendrá que implantar un registro de accesos a los datos, medida que hasta la fecha sólo se exigía a los ficheros considerados como de nivel alto.

3.11.2. Delitos contemplados en el Código Penal.

El propio Código Penal Español tipifica distintos delitos relacionados con el apoderamiento, utilización o modificación de datos, así como por su revelación a terceros o por el incumplimiento del deber de secreto, tal y como se recoge en los siguientes artículos del citado Código:

- Artículo 197.2: Se impondrán penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

- Artículo 197.3: Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos (...). Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

- Artículo 197.5: Cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

- Artículo 199 (Incumplimiento del deber de secreto): el profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

3.12. La problemática de la adaptación a la LOPD.

Tal y como ya se ha comentado en un apartado anterior, la LOPD define, con diferencia, el régimen sancionador más severo de toda la Unión Europea en materia de protección de datos de carácter personal. Así, podríamos citar algunos ejemplos de la gravedad de estas sanciones, basados todos ellos en ejemplos reales de sanciones impuestas por la Agencia de Protección de Datos a empresas españolas que incumplieron algunos de los preceptos de la LOPD:

- No inscribir ficheros con datos de carácter personal supone una infracción leve, con una sanción mínima de 601 euros.

- Un tratamiento de datos no consentido representa una infracción grave, con una sanción mínima de 60.101 euros. En este sentido, situaciones bastante habituales en la actualidad que podrían representar un tratamiento de datos no consentido serían algunas de las que se exponen a continuación (basadas en ejemplos de sanciones reales impuestas por la Agencia de Protección de Datos):

    - El envío de una carta a posibles clientes de una empresa que hayan sido localizados a partir de listines telefónicos ya caducados, es decir, listines telefónicos que hayan sido actualizados mediante nuevas ediciones impresas, las cuales, según el artículo 28.3 de la LOPD, anulan el carácter de fuente accesible de las ediciones anteriores.

    - La obtención de datos a partir de listados y bases de datos supuestamente públicos (el hecho de que se puedan obtener, por ejemplo, a través de una página Web, no quiere decir que tengan la consideración de fuente pública) o a través de otras fuentes (tener conocimiento de que un determinado ciudadano ha tenido un accidente de tráfico y ofrecerle mediante una carta personalizada los servicios de la empresa, por citar otro ejemplo basado en un caso real).

    - La inclusión de la fotografía de algún empleado o persona relacionada con una empresa en sus folletos, catálogos o páginas Web, sin contar con su consentimiento previo (ya que en este caso se estaría excediendo el marco de la relación laboral, por ejemplo, si se tratase de un empleado).

    - La modificación de los datos de un cliente (domicilio, número de cuenta…) sin poder probar que se contaba con su consentimiento para realizar dicha modificación, situación típica que se podría producir si se aceptase una petición de modificación mediante una simple llamada telefónica que no hubiera sido autentificada ni registrada.

- Mantener inexactos los datos de los clientes, empleados y/o proveedores de una empresa podría suponer una sanción mínima de 60.101 euros, correspondiente a una infracción grave. Asimismo, si el fichero con datos de carácter personal pierde la finalidad originaria, no se permite su reutilización para otras actividades, por lo que sus datos deberían ser destruidos, ya que en caso contrario también se podría imponer una sanción mínima de 60.101 euros.

- Compartir bases de datos entre distintas personas jurídicas (por ejemplo, entre empresas con distinto CIF pero integradas en un mismo grupo empresarial) supone una cesión de datos no consentida, lo que representa una infracción muy grave de la LOPD, con una sanción mínima de 300.505 euros.

- Ubicar copias de datos de carácter personal (como las direcciones de correo electrónico, por ejemplo) en servidores de países que, como Estados Unidos, no tienen un nivel de protección equiparable al de la Unión Europea, puede representar una sanción mínima de 300.505 euros, ya que si no se cuenta con el consentimiento previo de los interesados

y de la autorización del Director de la Agencia de Protección de Datos se considera una infracción muy grave.

- La LOPD obliga a la implantación de importantes medidas de seguridad tanto de carácter técnico como organizativo a las empresas que lleven a cabo tratamientos de ficheros con datos personales. El incumplimiento de estas medidas de seguridad puede ser objeto de una sanción por parte de la Agencia de Protección de Datos, de carácter grave o muy grave, por lo que a la empresa o institución responsable le podría ser impuesta una multa de entre 60.101 y 601.012 euros, dependiendo del nivel de seguridad del fichero de datos de carácter personal y de la gravedad de la infracción. Así, por ejemplo, la Agencia de Protección de Datos ha impuesto importantes sanciones a empresas que no han protegido de forma adecuada sus bases de datos (en algunos casos éstas se podían consultar a través de páginas Web, debido a un agujero de seguridad en su sistema informático).

- Los ficheros que puedan incluir datos relativos a la salud de las personas se consideran ficheros de nivel alto, por lo que se les deberían aplicar todas las medidas previstas en el Reglamento de Medidas de Seguridad. En España la Agencia de Protección de Datos considera que los ficheros de nóminas serán de nivel alto si incluyen datos relativos a cuotas sindicales o el registro de minusvalías físicas a efectos del cálculo de la retención del IRPF, datos que en la práctica deben registrar la mayoría de estos ficheros para cumplir con las obligaciones laborales y fiscales.

- Por otra parte, muchas empresas pueden estar recogiendo datos especialmente protegidos sin ser conscientes de sus implicaciones: hoteles y restaurantes que registren información sobre posibles dolencias o problemas de salud de sus clientes para ofrecerles dietas personalizadas; gimnasios que reflejen posibles discapacidades o problemas físicos de sus socios para tener previsto cualquier tipo de incidencia relacionada con su salud; concesionarios de automóviles que deben tramitar el impuesto de matriculación de personas discapacitadas (que se encuentran exentas de dicho impuesto, pero que deben acreditarlo con un justificante médico); centros de enseñanza que puedan recoger certificados médicos de los alumnos para justificar determinar ausencias a clase o a exámenes; etc.

- Las medidas de seguridad también afectan a los ficheros en papel. De hecho, la Agencia de Protección de Datos ha sancionado por la comisión de una infracción grave a empresas que tiraron directamente a la basura (sin destruir) los currícula vitae de candidatos presentados a un proceso de selección personal. Estas sanciones alcanzaron los 300.505 euros en el caso de clínicas privadas que no habían protegido de forma adecuada los historiales clínicos de sus pacientes (en algunos casos aparecieron los historiales de los pacientes en plena calle en un contenedor de la basura).

Convendría tener en cuenta, además, que en un mismo expediente sancionador se pueden aplicar varias de estas sanciones, como consecuencia de haber incumplido distintos preceptos de la LOPD.

De hecho, numerosos expertos han criticado la falta de proporcionalidad de las sanciones previstas por la LOPD. Así, por ejemplo, el Código Penal Español contempla penas de arresto de uno a tres fines de semana y multa de 20 euros a 12.000 por la falta de golpear o maltratar a alguien sin llegar a lesionarle. Sin embargo, la cesión no consentida de sus datos personales puede acarrear una sanción de hasta 601.012 euros para la empresa responsable.

Muchas empresas desconocen actualmente esta situación, por lo que se produce un elevado nivel de incumplimiento, sobre todo entre las empresas de menor dimensión. El propio Director de la Agencia Española de Protección de Datos estimaba recientemente que este nivel de incumplimiento superaba el 90% en el caso de las PYMES.

En la práctica son bastante frecuentes situaciones como las que se reflejan en las siguientes frases, que representan errores comunes que se plantean en las empresas y en algunos organismos públicos: "yo no tengo datos personales en mi empresa..."; "en mi empresa tenemos pocos datos..."; "ya hemos registrado los ficheros y con eso estamos cubiertos..."; "de los ficheros de datos se encarga nuestra gestoría..."; "esta Ley no debe ser muy importante, ya que no he oído hablar de ella..."; "esta Ley sólo afecta a las grandes empresas..."; "realmente esas multas no las paga nadie..."; etc.

Como consecuencia, observamos en la actualidad que en muchas empresas y en un porcentaje muy elevado de ayuntamientos y otros organismos públicos no se han inscrito todos los ficheros con datos de carácter personal; no se informa a los ciudadanos del tratamiento que se va a realizar con sus datos personales; no se han implantado todas las medidas de seguridad exigidas por la LOPD para proteger los ficheros; en bastantes casos todavía no se solicita consentimiento para realizar un tratamiento de datos de carácter personal; no se han formalizado los tratamientos encargados a terceros mediante un contrato; etc.

- Falta de sensibilización de los responsables, que en muchos casos no son conscientes de la importancia de la seguridad informática y de la necesidad de cumplir con el entorno legal (LOPD).
- Poca información disponible sobre la LOPD, a pesar de que entró en vigor en enero de 2000 y que define el marco sancionador más severo de toda la Unión Europea.
- Falta de medios informáticos para implantar las medidas de seguridad, sobre todo en las PYMES.
- Escasa formación en materia de seguridad informática.

Tabla 6: *Principales obstáculos para el cumplimiento del marco legal en materia de protección de datos*

3.13. Recomendaciones prácticas.

Para concluir este documento, se presenta un decálogo de recomendaciones para facilitar la adaptación y el cumplimiento de los requisitos del actual marco legal en materia de protección de datos tanto en las empresas como en los organismos públicos:

1. Sensibilización de los responsables de la organización sobre la importancia de cumplir con esta normativa y de reforzar la seguridad de sus datos y de su sistema informático. Sin el convencimiento y el apoyo decidido de estas personas, será muy difícil disponer de los recursos necesarios (inversión en equipamiento, tiempo de las personas directamente implicadas, etc.) para acometer con éxito el proyecto de adaptación a la LOPD.

2. Realizar una auditoría de partida:

    a. Revisión de los tratamientos de datos que se estén llevando a cabo o se prevean realizar a corto plazo: bases de datos y aplicaciones informáticas internas, así como tratamientos que se hayan subcontratado a terceros.

    b. Análisis de los ficheros con datos de carácter personal, ya sean bases de datos, documentos de aplicaciones ofimáticas (Word, Excel, etc.) o documentos en papel: cuál es su estructura (qué datos se están utilizando), su finalidad (para qué se emplean), procedencia (cómo se obtienen), actualización de los datos, tiempo previsto para su conservación, etc.

3. Inscripción de los ficheros identificados en el Registro General de Protección de Datos.

4. Elaboración del Documento de Seguridad adecuado al tipo de ficheros con datos de carácter personal sometidos a tratamiento por parte de la organización.

5. Implantación en la práctica de las Medidas de Seguridad contempladas en el Documento de Seguridad.

6. Revisión de posibles tratamientos y de cesiones de los datos a terceros.

    a. Formalización mediante un contrato de los tratamientos, exigiendo la implantación de las medidas de seguridad adecuadas y estableciendo expresamente que el encargado del tratamiento únicamente podrá tratar los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará para otra finalidad distinta, ni los comunicará, ni siquiera para su conservación, a otras personas y que dichos datos tendrán que ser eliminados de forma segura por el encargado del tratamiento una vez haya concluido su trabajo.

    b. Prestar especial atención a las cesiones: ¿qué datos se van a ceder? (proporcionalidad), ¿para qué? (finalidad) y ¿por qué? (legitimidad). Comprobar que siempre se cuenta con

el consentimiento del afectado o bien que se cumple alguna de las excepciones previstas por la LOPD para poder realizar la cesión sin que exista un consentimiento previo.

7. Revisión de los procedimientos relacionados con la protección de los datos y el cumplimiento de los derechos de los ciudadanos:

   a. Información a los interesados sobre el tratamiento de sus datos de carácter personal.

   b. Petición del consentimiento para el tratamiento.

   c. Respuesta a las peticiones de acceso, rectificación, cancelación u oposición, etc.

8. Formación y sensibilización de los empleados, aspecto que creemos fundamental, debido a la importancia del factor humano para evitar la mayoría de las infracciones graves y muy graves previstas por la LOPD: cesiones de datos no consentidas a otras empresas e instituciones, creación de nuevos ficheros sin el conocimiento de la organización, incumplimiento de las medidas de seguridad, etc.

9. Clara definición de las funciones y obligaciones del personal.

10. Otras cuestiones a considerar:

    a. Posibles transferencias internacionales de datos.

    b. Auditorías periódicas de las medidas de seguridad implantadas.

    c. Aplicación de regulaciones sectoriales específicas sobre protección de datos (sería necesario consultar para ello las instrucciones y recomendaciones dictadas por la propia Agencia de Protección de Datos).

En lo que se refiere a la identificación y posterior inscripción de los ficheros con datos de carácter personal, hay que tener en cuenta que la Ley Orgánica de Protección de Datos de Carácter Personal define un **fichero** como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

Además, en el artículo 2c) de la Directiva 95/46/CE se aclara la referencia a la forma de creación, almacenamiento, organización y acceso del fichero, al indicar que el conjunto de datos tendrá esa consideración "ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

En consecuencia, de lo establecido en la Directiva Europea y en la propia Ley Orgánica y, citando textualmente la opinión de la Agencia Española de Protección de Datos[2], "parece desprenderse que el concepto de fichero no va directamente vinculado a la exigencia de que el mismo se encuentre en una única ubicación, sino que será posible la existencia de ficheros distribuidos en lugares geográficos remotos entre sí, siempre y cuando la organización y sistematización de los datos responda a un conjunto organizado y uniformado de datos".

[2] Informe Jurídico 368/2003 de la Agencia Española de Protección de Datos.

Sin embargo, creemos que muchas empresas e instituciones han complicado innecesariamente la gestión de sus ficheros al declarar como un fichero independiente todas y cada una de las tablas de datos y documentos manejados en su sistema informático, aún cuando se refieran al mismo tipo de persona física, formalizando de este modo la inscripción de un gran número de ficheros ante la Agencia de Protección de Datos, con todo el papeleo que ello supone, además de la mayor complejidad en la gestión y actualización de estas declaraciones de ficheros.

Los ficheros con datos de carácter personal típicos de una empresa serían los relativos a sus clientes, proveedores, empleados (pudiendo distinguir entre el fichero de personal, de nivel básico, del de nóminas, de nivel alto y con acceso más restringido), contactos con terceros (potenciales clientes, direcciones de correo registradas en el programa de correo electrónico, etc.) o candidatos a empleo (base de datos de currícula vitae recibidos en la empresa), por citar los más habituales.

Por su parte, en un ayuntamiento los ficheros con datos de carácter personal más comunes serían el padrón municipal, empleados (pudiendo distinguir entre el fichero de personal, de nivel básico, del de nóminas, de nivel alto y con acceso más restringido), terceros de contabilidad (para gestión de cobros y pagos), beneficiarios de servicios sociales (generalmente de nivel alto), infractores, contactos con terceros, registro de usuarios de ciertos servicios municipales (bibliotecas, instalaciones deportivas, etc.), registro de bodas y parejas de hecho, registro de expedientes administrativos que afecten a ciudadanos, etc.

Así, por ejemplo, teniendo en cuenta que muchos de los ficheros de contactos de una empresa u organización comparten la misma estructura de datos (nombre y apellidos de la persona, empresa u organismo en el que trabaja, cargo, dirección, teléfono, dirección de correo electrónico, observaciones) y la misma finalidad del tratamiento (mantener el contacto con terceros), así como la relación de usuarios autorizados para acceder a sus datos dentro de la organización, creemos que sería recomendable su integración en, a ser posible, un único fichero. En principio, recomendamos evitar que en un mismo departamento o delegación de una empresa existan varios ficheros de contactos (salvo que incluyan datos distintos y se traten con diferentes finalidades) y que para cada evento o tipo de entidad exista un fichero de contactos específico[3].

También hay que tener en cuenta, por otra parte, que la existencia de multitud de ficheros de contactos aislados e inconsistentes entre sí podría provocar que una misma persona figure con datos distintos y, en algunos casos, con datos desactualizados, en las distintas bases de datos de contactos, incumpliendo el principio de calidad de los datos que establece la Ley Orgánica de Protección de Datos. Es decir, si un ciudadano solicitase al responsable del fichero que se actualizasen sus datos personales, la existencia de multitud de ficheros de contactos dificultaría en gran medida esta actualización, ya que tendría que ser realizada de forma aislada por cada departamento o delegación de la empresa.

[3] La situación sería equivalente, por poner un símil, al de una empresa que deseara registrar varios ficheros de clientes en función del tipo de cliente o de su ubicación geográfica, en lugar de un único fichero de clientes.

Por este motivo, consideramos conveniente evitar que los propios usuarios puedan crear sus propios listados de personas de contacto en documentos de Word o en libros de Excel para poder realizar un *mailing*, por ejemplo, para promocionar determinados eventos o actividades, salvo cuando se trate de ficheros temporales extraídos de la base de datos de contactos de la organización, que se destruyan una vez realizado el tratamiento puntual.

Creemos, por lo tanto, conveniente definir una política interna que permita organizar y gestionar los contactos de todo tipo (institucionales, comerciales, de interesados en actividades de la organización, de medios de comunicación, etc.), aplicando en la medida de lo posible el principio de "dato único", para evitar que una misma persona pueda figurar con datos distintos en diferentes bases de datos. Además, los propios empleados no deberían crear nuevos ficheros sin la autorización correspondiente de su departamento.

Del mismo modo, los ficheros que puedan estar ubicados en delegaciones, si tienen la misma estructura y cuentan con la misma finalidad que los que se encuentran ubicados en la sede principal de la organización, se podrían considerar como integrados dentro del mismo fichero.

Por otra parte, consideramos que se debería evitar, en la medida de lo posible, incluir datos especialmente protegidos relativos a la salud de las personas en algunas bases de datos, para no tener que aplicar las medidas de seguridad de nivel alto y estar expuestos a las sanciones más elevadas por el incumplimiento de los preceptos de la LOPD.

Asimismo, para poder cumplir con el requisito de información y de solicitud de consentimiento, en los cuestionarios, páginas Web y formularios impresos deberían figurar, en forma claramente legible, cláusulas informativas y de solicitud del consentimiento para el tratamiento, como la que se muestra a continuación:

> *"De conformidad con lo establecido en la LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPD), se informa al interesado que estos datos se incorporan al fichero automatizado propiedad de la organización **XXX**, denominado fichero **ZZZ**, con domicilio en _____. Usted podrá ejercer, en cualquier momento, los derechos de acceso, rectificación, cancelación y oposición, previstos por la Ley. Al firmar este documento autoriza la utilización de sus datos personales exclusivamente para el fin solicitado."*

Tabla 7: Ejemplo de cláusula para dar cumplimiento al derecho de información.

Del mismo modo, para obtener el consentimiento en la cesión de datos a otras instituciones, se podrían añadir otros párrafos informativos a la cláusula anterior, como los que se citan a continuación:

"El interesado acepta que sus datos puedan ser cedidos a otras empresas del grupo, exclusivamente para la finalidad prevista para este fichero automatizado", cláusula típica para compartir datos de clientes o de candidatos de empleo entre distintas sociedades de un mismo grupo empresarial.

"El interesado consiente que se puedan ceder sus datos a cualquier otra entidad cuya intervención sea necesaria o conveniente en la realización de operaciones conexas y necesarias a los fines propios de la relación contractual o negocial. El presente consentimiento se otorga sin perjuicio de todos los derechos que asisten al interesado en virtud de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal".

Tabla 8: *Ejemplos de cláusulas para solicitar el consentimiento para poder ceder los datos del interesado a otras instituciones.*

Por otra parte, en lo que se refiere a las auditorías periódicas sobre la seguridad informática, el nivel de protección de los ficheros con datos de carácter personal y el cumplimiento de lo dispuesto por la LOPD, que se tienen que realizar por lo menos cada dos años en aquellas organizaciones con ficheros de nivel medio o alto, los principales aspectos que tendrían que ser verificados en dicha auditoría son los que se presentan a continuación:

- Revisión de las características técnicas del sistema informático de la organización: locales y puestos de trabajo, equipamiento hardware, software y aplicaciones informáticas, infraestructura de red y de comunicaciones.
- Comprobación de que la lista actualizada de usuarios que tienen acceso a los ficheros se corresponde con la lista de los usuarios realmente autorizados por el responsable de los ficheros.
- Verificación de la existencia del registro de incidencias y revisión de las incidencias registradas en los últimos meses por la organización para que, independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, se puedan adoptar las medidas correctoras que limiten esas incidencias en el futuro.
- Revisión de la adecuada gestión de los soportes informáticos.
- Comprobación de la existencia de copias de respaldo que permitan la recuperación de los datos de los ficheros, así como de la correcta realización del procedimiento periódico de generación de copias de seguridad.
- Revisión del procedimiento de registro y autorización de entradas y salidas de datos de carácter personal, ya sea por red o por medio de algún soporte informático.

- Verificación de las medidas de seguridad físicas, técnicas y organizativas implantadas por la organización, tanto en los ficheros principales como en los ficheros temporales que puedan estar siendo utilizados por los empleados.

- Evaluación del nivel de sensibilización y de formación de los usuarios con acceso a datos de carácter personal.

- Comprobación de la existencia de tratamientos de datos encargados a terceros: regulación mediante un contrato de prestación de servicios, que incluya las correspondientes cláusulas de seguridad y protección de datos.

- Existencia de cesiones de datos a otras personas jurídicas, así como de posibles transferencias internacionales de datos.

- Evaluación del cumplimiento de la obligación de información del tratamiento de datos de carácter personal a los afectados, así como del cumplimiento de sus derechos de acceso, rectificación, cancelación y oposición.

Capítulo 4

4. Cuestiones sobre la LOPD en la Administración Local[4]

Pregunta 1: ¿En un ayuntamiento, quién es el responsable de un fichero con datos personales?

En los ficheros públicos, el responsable del fichero es el órgano administrativo que trata la información y tiene competencias en la materia. El responsable de un fichero debe indicarse expresamente en el correspondiente anexo de la ordenanza en la que se crea el mismo.

Pregunta 2: ¿Puede un ciudadano oponerse al tratamiento de sus datos personales por parte del ayuntamiento?

Aunque el derecho de oposición está reconocido en la Ley Orgánica de Protección de Datos (LOPD), no puede ser ejercido cuando los datos sean tratados por un ayuntamiento (o en general por cualquier otra administración pública) siempre que sea para el ejercicio de sus competencias, dado que precisamente ésta es una de las excepciones legales a la norma general del consentimiento.

Pregunta 3: ¿Pueden los concejales acceder a datos de carácter personal albergados en ficheros del ayuntamiento?

Los concejales, en cuanto miembros de las Corporaciones locales, tienen la condición de poderes públicos y la obligación de promover la participación de todos los ciudadanos en la vida política, económica y cultural, para lo cual tienen el derecho a obtener del Alcalde, Presidente o Comisión de Gobierno de la Corporación cuanta información precisen.

[4] Este apartado ha sido elaborado tomando como referencia algunas de las consultas resueltas y de los informes jurídicos elaborados por la Agencia Española de Protección de Datos (www.agpd.es), así como de la sección de consultas disponible en la página Web de la Agencia de Protección de Datos de la Comunidad de Madrid (www.apdcm.es).

Podrán acceder a los datos solicitados (incluidos los albergados en el padrón) sin previo consentimiento de los afectados cuando dicho acceso sea necesario para el desarrollo de sus funciones de control de la Corporación en los términos previstos en la Ley de Bases de Régimen Local. Es imprescindible que en la petición efectuada por el concejal se determine la finalidad de la cesión de datos, así como que se entregue el mínimo de datos necesario sobre el mínimo número de personas que permita alcanzar la finalidad del acceso.

De igual forma, no pueden utilizarse los datos del padrón para funciones distintas de las municipales. Así, sería incompatible utilizar el padrón municipal para que el Alcalde envíe una carta a los vecinos para felicitarles por su onomástica o por el nacimiento de su hijo.

El acceso a la información por parte de los miembros de la Corporación municipal debe regirse siempre por la obligación de reserva, tal como se dispone en el artículo 16 del Real Decreto 2568/1986, de 28 de noviembre, de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, que además impone un modo de actuación determinado.

Pregunta 4: ¿Se deben ceder datos del padrón municipal de habitantes a otras Administraciones Públicas (como la Comunidad Autónoma, Ministerios, etc.)?

Los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes.

Pregunta 5: ¿Se pueden ceder datos del padrón municipal a personas físicas o jurídicas de naturaleza privada?

La cesión de este fichero o de otros de titularidad pública a personas físicas o jurídicas de naturaleza privada no está autorizada por la Ley Orgánica de Protección de Datos ni está prevista en la Ley de Bases de Régimen Local. Sólo se podría llevar a cabo la cesión si se tuviera el consentimiento expreso e informado de los ciudadanos afectados.

Pregunta 6: ¿Se pueden utilizar los datos de los ciudadanos que figuran en las guías telefónicas para crear un fichero de contactos y realizar "*mailings*"?

La legislación vigente sobre protección de datos considera que los datos personales básicos que figuran en los repertorios telefónicos (nombre, apellidos, y dirección) son fuentes de acceso directo al público y, en consecuencia, pueden ser utilizados sin necesidad de contar con el consentimiento expreso del interesado.

Observaciones al respecto:

1. A pesar de no ser necesario el consentimiento para el tratamiento, cuando se realice el "*mailing*" se tendrá que informar al interesado acerca del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

2. Las guías telefónicas impresas en papel pierden su condición de fuente accesible al público en el momento en que se publique una nueva edición.

Pregunta 7: ¿Se pueden facilitar los datos del catastro a personas distintas del titular de los mismos?

Para poder acceder a los datos nominativos del catastro y obtener documentación de los mismos, es necesario disponer del consentimiento expreso y por escrito del titular de éstos, salvo que se den las excepciones o se tenga la condición de interesado en la forma descrita en el Real Decreto 1485/1994 que establece las normas para acceso y distribución pública de dicha información.

Fuera de estos supuestos únicamente se podrá acceder a los datos del catastro debidamente disociados, es decir un acceso donde no conste ninguno de los datos protegidos referidos al nombre, apellidos, razón social, código de identificación y domicilio de quienes figuren inscritos en el Catastro como titulares o sujetos pasivos del Impuesto sobre Bienes Inmuebles, así como el valor catastral y los valores del suelo y, en su caso, de la construcción, de los bienes inmuebles individualizados.

Pregunta 8: ¿Qué requisitos hay que cumplir para poder encargar a una empresa o institución externa al ayuntamiento un tratamiento de datos en el que se tengan que manejar datos de carácter personal?

En este caso no es preciso el consentimiento individual de cada uno de los vecinos o ciudadanos, pero en virtud de lo dispuesto en el artículo 12 de la LOPD, sí debe existir un contrato específico entre el ayuntamiento y la empresa o institución externa que contemple expresamente que el encargado del tratamiento únicamente tratará los datos personales conforme a las instrucciones del ayuntamiento, que no los utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas u organizaciones. En el contrato habrán de estipularse también las medidas de seguridad que aplicará la entidad o empresa externa en relación con los datos personales que está tratando.

Por lo que respecta al período de conservación de los datos, el artículo 12.3 establece que "una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

Por otra parte, según el artículo 12.4, "en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente", siendo, en consecuencia, de aplicación el régimen sancionador establecido en los artículos 43 y siguientes de la LOPD.

En cuanto a la obligación de notificación del tratamiento, deberá efectuarse por el responsable del mismo (en este caso el propio Ayuntamiento), indicando la existencia de una entidad encargada del tratamiento, debiendo además hacerse constar expresamente la ubicación del fichero.

Pregunta 9: ¿Se puede contratar la gestión del fichero del Padrón municipal con una empresa privada?

De conformidad con lo previsto en el artículo 17.1 de la Ley de Bases de Régimen Local, la formación, mantenimiento, revisión y custodia del Padrón municipal corresponde al Ayuntamiento, que además tiene la obligación de gestionarlo por medios informáticos.

En el supuesto de que no dispongan de capacidad económica para la gestión informática del Padrón, la misma se realizará por la Diputación Provincial.

Pregunta 10: ¿Qué documentación específica es exigible en los "contratos menores" que incluyan en su objeto el tratamiento de datos de carácter personal?

Si bien con carácter general la formalización de un contrato menor puede realizarse simplemente a través de una factura, comprobante o recibo, cuando se utilice para tramitar la contratación de bienes o servicios que impliquen el tratamiento de datos personales de la Administración contratante por parte del contratista, debe existir un documento contractual elaborado con anterioridad a la realización del servicio contratado que desarrolle las obligaciones establecidas en el artículo 12 de la Ley Orgánica de Protección de Datos de Carácter Personal, y el sometimiento a ellas por el contratista.

El clausulado habrá de incluir, en particular, que el contratista tratará los datos exclusivamente según le indique la Administración contratante, que no los utilizará con fin distinto al que figure en el contrato, que no los comunicará a terceros, así como las medidas de seguridad correspondientes.

Pregunta 11: ¿Qué consideración tienen los ficheros de una Empresa Municipal que se ha constituido como una Sociedad Anónima con capital 100% propiedad del ayuntamiento?

Aunque el capital sea de titularidad íntegramente municipal, los ficheros de datos personales de empresas y otras organizaciones con personalidad jurídica propia que estén sometidas al Derecho Privado han de ser declarados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos como ficheros de titularidad privada, estando sometidas, por lo tanto, al régimen de importantes sanciones económicas previstas por la LOPD.

Pregunta 12: ¿Puede el Ayuntamiento publicar en Internet o en otros medios las actas de plenos y reuniones de la junta de gobierno local cuando éstas contengan datos de carácter personal?

Las actas de los Plenos se podrán publicar en Internet sin consentimiento de las personas cuyos datos aparecen en las mismas si así lo determina expresamente el Reglamento Orgánico del Ayuntamiento y la información con datos de carácter personal que contengan no afecte al honor, a la intimidad personal o familiar y a la propia imagen de los afectados. Sin embargo, no se podrían publicar las actas de la Junta de Gobierno Local.

Esto es así porque el artículo 70 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, que ha sido modificada recientemente por la Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local, establece que las sesiones del Pleno de las Corporaciones Locales son públicas, salvo en aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos a que se refiere el artículo 18.1 de la Constitución, cuando así se acuerde por mayoría absoluta. Sin embargo, las sesiones de la Junta de Gobierno Local no son públicas.

Pregunta 13: ¿Puede una Administración Autonómica o de ámbito Estatal ceder datos de familias numerosas a los Ayuntamientos sin el consentimiento de los interesados para una finalidad fiscal (por ejemplo, para comprobar si ha de renovarse o no un beneficio fiscal en el Impuesto de Bienes Inmuebles derivado de dicha condición)?

Sí, es posible esta cesión, a tenor de lo previsto en el artículo 94 de la Ley 58/2003 de 17 de diciembre, General Tributaria (en vigor desde el 1 de julio de 2004), referido al deber de informar y colaborar con la Administración Tributaria y en concreto a lo previsto en su apartado 1, párrafo primero:

"Las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos del Estado, de las Comunidades Autónomas y de las entidades locales; los organismos autónomos y las entidades públicas empresariales; las cámaras y corporaciones, colegios y asociaciones profesionales; las mutualidades de previsión social; las demás entidades públicas, incluidas las gestoras de la Seguridad Social y quienes, en general, ejerzan funciones públicas, estarán obligados a suministrar a la Administración tributaria cuantos datos, informes y antecedentes con trascendencia tributaria recabe ésta mediante disposiciones de carácter general o a través de requerimientos concretos, y a prestarle, a ella y a sus agentes, apoyo, concurso, auxilio y protección para el ejercicio de sus funciones."

Termina este artículo 94 con un quinto apartado estableciendo que: "La cesión de datos de carácter personal que se deba efectuar a la Administración tributaria conforme a lo dispuesto en el artículo anterior, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado."

Pregunta 14: ¿Puede la Policía Local ceder datos personales relacionados con accidentes de circulación a compañías aseguradoras?

La Policía Local puede facilitar los datos personales referidos a un accidente de circulación a las compañías de seguros que actúen en calidad de parte interesada en el mismo, puesto que éstas reúnen los requisitos para acogerse a las excepciones recogidas en el artículo 11.2 a) y 11.2.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En este caso la cesión de datos constituiría una de las excepciones a la petición del consentimiento al afectado, ya que la finalidad de esta actuación por parte de la policía local sería dar a conocer a los implicados en el accidente la identidad de los contrarios, todo ello, para posibilitar el cumplimiento de lo previsto en el artículo 129 del Real Decreto 1428/2003 por parte de las partes implicadas, que, como consecuencia del accidente van a mantener una relación jurídica civil, penal, administrativa, etc.

Asimismo, la excepción del artículo 11.2 a) de la LOPD vendría amparada en el artículo 35 de la Ley 30/1992, según el cual "los ciudadanos, en sus relaciones con las Administraciones Públicas, tienen los siguientes derechos: a) A conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados, y obtener copias de documentos contenidos en ellos…."

En ambos casos, es imprescindible que las compañías aseguradoras acrediten debidamente la representación de sus asegurados, y éstos tengan un interés legítimo y directo en el accidente.

Pregunta 15: ¿Pueden crearse y utilizarse ficheros que contengan datos de carácter personal sin que se haya publicado la disposición en la que se crean?

No. La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal tipifica como infracción grave "proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin la existencia de una autorización de disposición general, publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente".

De igual manera, la LOPD tipifica como infracción leve, cuando no sea constitutivo de infracción grave, "no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos".

Pregunta 16: ¿Los datos recogidos para una determinada finalidad pueden utilizarse para cualquier otra que se pueda plantear a posteriori?

Los datos sólo se pueden recabar para cumplir una finalidad determinada, explícita y legítima, que además deberá conocer el interesado, como regla general, con carácter previo a la recogida de sus datos.

En consecuencia, no podrán utilizarse los datos recogidos para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos, aunque la recomendación normal es que estas tareas se realicen con datos disociados (eliminando cualquier dato que identifique o permita identificar a las personas).

Pregunta 17: ¿Es posible denegar el ejercicio del derecho de acceso que la LOPD reconoce a los ciudadanos por la dificultad o el elevado coste que puede suponer su ejercicio?

No. La LOPD ya prevé (y ya lo preveía la LORTAD desde 1992), que los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

No obstante, la LOPD limita el ejercicio de ese derecho a los ciudadanos, pudiendo ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Pregunta 18: ¿Cómo se puede dar cumplimiento al deber de información al ciudadano, que establece la LOPD, con carácter previo a la recogida de sus datos?

Para dar cumplimiento a este deber de información pueden utilizarse diferentes medios: uno de los que propone la LOPD es la inclusión de textos informativos en los impresos y cuestionarios que se utilicen. De modo complementario pueden colocarse carteles informativos, accesibles a los ciudadanos, en los puntos en que se realice la recogida de los datos.

Debe analizarse en cada supuesto concreto, la forma de recogida de los datos, la naturaleza del colectivo del que se están recogiendo (menores, mayores, discapacitados, etc.) y la forma más efectiva para que se dé cumplimiento al deber establecido en la Ley.

Pregunta 19: ¿Puede cualquier empleado de un ayuntamiento acceder a todos los datos que puedan existir en los ficheros de esta Administración Local?

No. Cada empleado podrá acceder, única y exclusivamente, a aquellos datos que necesite manejar en el ejercicio de la actividad que tiene encomendada, para conseguir la finalidad perseguida.

No todas las personas que constituyen una organización deben acceder a todos los datos: sólo deberán tener acceso a aquéllos que cumplan el principio de calidad (adecuados y no excesivos) para la finalidad que tenga encomendada.

Pregunta 20: ¿Sería posible una cesión de datos de familiares de una persona fallecida realizada desde un hospital público a una empresa privada de servicios funerarios, con el objeto de ofertarles los servicios de dicha empresa?

En esta situación no rige ninguna de las excepciones previstas en el artículo 11.2 de la LOPD para la cesión o comunicación de datos personales a terceros, siendo necesario, por tanto, el disponer del consentimiento expreso e inequívoco de los afectados, quienes tendrán que ser informados previamente de la posible cesión de sus datos a la empresa de servicios funerarios.

Este tipo de actuaciones, caso de realizarse sin el consentimiento de los afectados, constituyen una de las infracciones más graves a la protección de datos y así vienen previstas en el artículo 44.4 b) de la LOPD.

Pregunta 21: ¿Es posible publicar en una página Web los datos de personas que participan en algún procedimiento selectivo: concesión de premios, etc.?

Un procedimiento administrativo de concurrencia competitiva está sujeto al principio de publicidad, siéndole de aplicación lo dispuesto en el artículo 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En dicho artículo se establecen las normas para notificar los actos administrativos, estableciendo en su apartado 6b que la publicación del acto sustituirá a la notificación en el caso de que se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo.

Asimismo, el artículo 45 del mismo texto legal, establece que las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establezcan la Constitución y las leyes.

La publicación de los resultados obtenidos por los distintos candidatos tiene la finalidad de hacer efectiva la práctica de la notificación del acto administrativo, que en este caso es el acta de calificación, y posibilitar que se puedan formalizar las oportunas reclamaciones contra dicho resultado ante el Tribunal. Dicha publicación en las correspondientes páginas Web daría cumplimiento a lo señalado en el artículo 45 de la Ley 30/1992, de 26 de noviembre, respetando en todo caso el principio de calidad de los datos, establecido en el artículo 4 de la LOPD

según el cual, los datos deberán ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

No obstante, a la hora de publicar los listados de calificaciones en la página Web se debería incluir el siguiente texto: "Los listados que se publican en esta página Web y que contienen datos de carácter personal se ajustan a la legislación actual de protección de datos y su única finalidad, de conformidad con lo previsto en el artículo 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, es la de proceder a notificar a cada uno de los aspirantes el contenido del procedimiento selectivo. Estos listados no constituyen fuente de acceso público y no podrán ser reproducidos ni en todo ni en parte, ni transmitidos ni registrados por ningún sistema de recuperación de información, sin el consentimiento de los propios afectados".

Pregunta 22: ¿Pueden acceder a la historia clínica de los pacientes de un centro de salud los asistentes sociales que prestan servicios en un ayuntamiento?

No podrán acceder a estos datos, salvo si cuentan con consentimiento expreso del paciente en cuestión, puesto que no son profesionales sanitarios ni personal de administración y gestión de los centros asistenciales, que son los únicos que tienen habilitación legal para acceder en el ejercicio de su actividad a los datos de la historia clínica sin consentimiento de los pacientes. Por tanto, la única posibilidad para que el asistente social pueda tener acceso a la historia clínica de un paciente será si cuenta con el consentimiento expreso de éste y además dicho acceso está justificado en una finalidad de carácter asistencial o social de interés para el propio paciente.

Pregunta 23: ¿Se puede publicar en Internet el directorio (nombres y datos profesionales de contacto) de todo el personal de un Ayuntamiento?

En la medida que la publicación de datos personales en páginas Web implicaría una cesión de datos indiscriminada, dicha cesión se regula por lo previsto en el artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En consecuencia y no existiendo habilitación legal que permita esta publicación, para hacerlo, sería necesario que cada afectado diera su consentimiento expreso e inequívoco, debiendo el Ayuntamiento asimismo permitir que en cualquier momento pudiese oponerse a la misma, procediendo al borrado y cancelación de sus datos del sitio Web del Ayuntamiento en Internet.

Igualmente, en este caso, habría que evitar que se pudiesen confeccionar listados del directorio por aquellos que accedan al mismo, dado que la finalidad del mismo es informativa y a estos efectos debería incluirse una cláusula a modo de advertencia, indicando de que los datos y direcciones de correo electrónico del Ayuntamiento que son objeto de publicación en el directorio "sirven únicamente a finalidades exclusivamente administrativas, y su empleo para cualquier uso distinto de los señalados, y en particular para fines comerciales o envío de correos basura, será contrario a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y será puesto en conocimiento de las autoridades competentes en materia de protección de datos".

Sí podría publicarse el directorio, sin necesidad de consentimiento por parte de los interesados, en la red interna o Intranet del Ayuntamiento, siempre y cuando el acceso esté limitado al resto de personal del Ayuntamiento, considerando que la cesión se efectuaría en el ámbito de la relación laboral o administrativa y que

la previsible finalidad de esa comunicación sería la de facilitar este tipo de relaciones. En este caso, la cesión (publicación) podría estar exceptuada de la prestación del consentimiento por aplicación de la excepción del artículo 11.2.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que señala que no será necesario el consentimiento para la sesión de datos, cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En cualquier caso, el Ayuntamiento debería cumplir igualmente con el deber de información contenido en el artículo 5.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Pregunta 24: ¿Las calificaciones académicas de los alumnos asistentes a una serie de cursos pueden publicarse en los tablones de anuncios del centro o en Internet?

Con carácter general, las notas de calificación de cada asignatura o curso tienen como destinatario los alumnos, anotándose en su expediente académico. En consecuencia la difusión de dichas notas de calificación a través de tablones de anuncios o de Internet constituye una cesión de datos de carácter personal de los alumnos.

En ese caso y atendiendo a la regulación de la LOPD sería necesario que cada alumno diera su consentimiento inequívoco para poder realizar la publicación de las calificaciones, dado que este supuesto no constituye ninguna de las excepciones legales para poder efectuar las cesiones sin consentimiento.

No hay que confundir la publicación de estas calificaciones con la posibilidad de publicar los listados de aspirantes con sus resultados de un proceso selectivo (tales como las pruebas de acceso a la Universidad, contratación de personal, etc.). En estos casos será posible la publicación ya que rige el principio de publicidad y así viene previsto específicamente en el artículo 59.5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Pregunta 25: ¿Los padres y tutores de los alumnos tienen derecho a solicitar las calificaciones académicas al centro o institución que organiza e imparte los cursos?

Si los alumnos son menores de edad, los padres y tutores tienen derecho a solicitar al centro las calificaciones académicas de sus hijos.

En el caso de que los alumnos sean mayores de edad, no se podrán ceder, ya que constituiría una cesión sin estar amparada por las excepciones que contempla la ley.

Pregunta 26: ¿Es posible realizar un tratamiento automatizado de la huella digital para la comprobación de la identidad de los funcionarios al servicio de un Ayuntamiento y el cumplimiento por los mismos de su jornada de trabajo?

Para resolver esa cuestión debemos analizar previamente cuál es la incidencia que los datos biométricos tienen en el ámbito de aplicación de la LOPD, siendo datos biométricos aquellos aspectos físicos que mediante un determinado análisis técnico permiten identificar a un determinado individuo (tales como las huellas digitales, el iris del ojo, la voz, etc.).

El artículo 3.a) de la LOPD, define los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables". En este sentido debe indicarse que, si bien el procesado de los datos biométricos no revela nuevas características referentes al comportamiento de las personas sí permite, lógicamente, su identificación, por lo que resulta evidente que, en caso de procederse a su tratamiento, éste deberá ajustarse a la LOPD. El problema consiste en determinar si el tratamiento de la huella digital puede ser considerado excesivo para el fin que lo motiva, atendiendo al principio de proporcionalidad consagrado por la Ley.

La Agencia Española de Protección de Datos ha considerado que los datos biométricos tienen la condición de datos de carácter personal y que, dado que los mismos no contienen ningún aspecto concreto de la personalidad, limitando su función a identificar a un sujeto cuando la información se vincula con éste, su tratamiento no tiene mayor trascendencia que el de los datos relativos a un número de identificación personal, como podría ser el DNI.

En cuanto a la posibilidad de que las huellas sean tratadas sin consentimiento del interesado, y teniendo en cuenta que el tratamiento tiene su origen, precisamente de la necesidad de asegurar el debido cumplimiento de las obligaciones derivadas de la relación estatutaria que vincula al funcionario o empleado con la Administración, será posible el tratamiento inconsentido, ya que el artículo 6.2 de la LOPD prevé que no será preciso el consentimiento cuando los datos "se refieran a las partes de un contrato o precontrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento".

En todo caso, el fichero quedaría sometido a las demás disposiciones de la LOPD, en cuanto a su creación y funcionamiento, siendo necesario informar a los interesados de su existencia y de los demás extremos a que se refiere el artículo 5.1 de la Ley Orgánica.

Pregunta 27: El dato de que una persona es fumadora; ¿entra dentro del concepto de dato de salud?

Esta cuestión no se especifica en el propio texto de la LOPD. Por este motivo, recurriendo a la postura de la Unión Europea sobre esta materia, podemos considerar que el apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa viene a definir la noción de 'datos de carácter personal relativos a la salud', considerando que su concepto abarca 'las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo', pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. Añade el citado apartado 45 que 'debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas'.

En este mismo sentido, la Recomendación nº R (97) 5, del Comité de Ministros del Consejo de Europa, referente a la protección de datos médicos, afirma que 'la expresión *datos médicos* hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas'.

Por otra parte, es evidente que no es lo mismo anotar en un fichero de control de pasajeros y billetes la condición o no de fumador de una persona (porque no se van a realizar posteriores evaluaciones médicas del mismo) que anotar dicha condición en un fichero de seguros de vida, en el que dicha anotación no va aislada, sino junto con otros datos de salud. En uno y otro caso, las finalidades para las que se va a usar esa anotación son diferentes.

En conclusión, si el dato de fumador o no fumador no sirve para realizar evaluaciones de salud o médicas, en principio, no parece que sea dato de salud, ya que, aunque sea un dato de riesgo potencial para la salud, no informa por sí solo del estado de salud pasado, presente o futuro de la persona. En caso contrario, sí será un dato de salud.

Pregunta 28: ¿Cuál es la naturaleza de los datos psicológicos a efectos de su tratamiento?

Resulta muy frecuente que en un Ayuntamiento se lleve a cabo un tratamiento de datos de carácter psicológico en el ámbito de sus competencias en materia de asistencia social, incluyendo determinados datos obtenidos de la apreciación subjetiva de las personas encargadas de llevar a cabo la realización material de encuestas, referentes a los "problemas" que presenta el perfil psicológico de los sujetos encuestados: tales como dificultades en el aprendizaje, alcoholismo, drogodependencia, ludopatía, conflictos de pareja, síntomas depresivos, conflictos de adaptación al medio familiar o social, desarraigo, etc.

En este contexto, los datos psicológicos deben ser considerados, a los efectos de la aplicación de la LOPD, como datos relativos a la salud de las personas. Para delimitar el fundamento de esta inclusión habrá de distinguirse entre los datos incorporados a historiales clínico-psiquiátricos o psicológicos y los no incorporados a los mismos.

No debe olvidarse que el tratamiento de datos de carácter psicológico podría, en la práctica, generar un perfil completo del individuo, del que se desprendiese el conocimiento de otros datos especialmente protegidos por el legislador, tales como las creencias morales y religiosas o la vida sexual del sujeto. Ello no hace sino ratificar la conclusión del necesario sometimiento de los datos de carácter psicológico al régimen de los datos relativos a la salud de las personas, consagrado por la LOPD.

Pregunta 29: ¿Cuál es la naturaleza de los datos sobre drogodependencias a efectos de su tratamiento?

En aplicación de la postura manifestada por la Unión Europea sobre esta cuestión (apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa, citado en la pregunta 27), el dato sobre la drogodependencia de una persona, necesariamente asociado a la asistencia social prestada por muchos Ayuntamientos, así como la indicación de la sustancia consumida, ha de ser considerado un dato relacionado con la salud, incluso en el supuesto de que el afectado no sufriera ningún tipo de dolencia.

Pregunta 30: ¿Se aplica la LOPD a los empresarios individuales o autónomos? ¿Y a las personas jurídicas? ¿Y a los datos de personas ya fallecidas?

Con carácter general, el objeto de la Ley está regulado en el artículo 2.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que expresamente establece:

Artículo 2. Ámbito de aplicación: La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Por ello, no le es de aplicación la Ley Orgánica 15/1999:

- A los datos de personas jurídicas.
- A los datos de las personas fallecidas, ya que el artículo 32 del Código Civil dispone que "la personalidad civil se extingue por la muerte de las personas", lo que determinaría, en principio, la extinción con la muerte de los derechos inherentes a la personalidad.

Por el contrario, sí le es de aplicación:

- A los datos de los empresarios individuales – personas físicas (autónomos).
- A los ficheros de empresas que tengan una relación de personas físicas de contacto, como Administradores, Gerentes, Comerciales, etc.

Pregunta 31: ¿La empresa o institución encargada de un tratamiento de datos de carácter personal debería declarar el fichero?

Como cuestión previa, es preciso indicar que en ningún caso las empresas que accedan a los datos personales para realizar un determinado tratamiento tendrán la consideración de responsables del fichero, siendo meros intermediarios para el completo cumplimiento del "objeto contractual previamente consentido por el afectado".

En caso contrario, esto es, cuando la empresa interviniente actuase en nombre propio, y no como mera mandataria de la entidad responsable del fichero, nos encontraríamos ante un supuesto de cesión o comunicación de datos de carácter personal, que sería lícito siempre que se contase con el consentimiento del afectado o que la transmisión de los datos fuera necesaria para el adecuado cumplimiento de la relación contractual que vincule al afectado con la entidad responsable del fichero.

En resumidas cuentas, el encargado de tratamiento no es responsable del fichero y, por lo tanto, no debe inscribirlo en el Registro General de Protección de Datos, si bien sí es responsable de aplicar las medidas de seguridad que correspondan al fichero en cuestión en función del nivel de seguridad de los datos de carácter personal.

Pregunta 32: ¿Es posible una subcontratación de servicios por parte del encargado del tratamiento de datos de carácter personal?

En lo referente a la posible subcontratación del servicio, el artículo 12.2 de la Ley Orgánica 15/1999 establece que en las estipulaciones del contrato debería hacerse constar que el encargado del tratamiento no comunicará los datos, "ni siquiera para su conservación, a otras personas".

Si se estableciera la posibilidad de subcontratar sucesivamente dicho tratamiento sin conocimiento del responsable, éste carecería de conocimiento para poder atender cualquier reclamación efectuada por el afectado e incluso para conocer quién accede en cada momento a los datos de carácter personal cuyo tratamiento ha sido consentido por el interesado.

Teniendo en cuenta la fundamentación anteriormente citada, sí sería posible la transmisión de los datos a un tercer subcontratista en caso de que el responsable pudiera conocer específicamente esta circunstancia. Ello se lograría bien mediante su participación directa en el contrato con el tercero, bien encomendando un apoderamiento a tal efecto al encargado del tratamiento, bien haciéndose constar expresamente en el contrato firmado entre el responsable y el encargado la propia circunstancia de la subcontratación.

Así lo ha declarado la Agencia Española de Protección de Datos en algunas de sus Recomendaciones, tal y como se recoge textualmente:

"Por otro lado, de preverse o producirse por parte del prestador de un servicio una subcontratación que implique tratamiento de datos personales deberá reflejarse en el contrato los requisitos exigidos por la normativa de protección de datos haciendo constar expresamente, además de las prescripciones del citado artículo 12 que, o bien el contratista del servicio actúa en nombre y por cuenta del responsable del fichero o tratamiento o, alternativamente, se especifiquen los siguientes requisitos acumulativos, que deberán figurar en el contrato:

a) Que los servicios a subcontratar se hayan previsto expresamente en la oferta o en el contrato celebrado entre el responsable del fichero y el encargado del tratamiento.

b) Que el contenido concreto del servicio subcontratado y la empresa subcontratista conste en la oferta o en el contrato.

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

En consecuencia, la subcontratación de terceras entidades encargadas del tratamiento será posible siempre y cuando o bien el contratista del servicio actúa en nombre y por cuenta del responsable del fichero o tratamiento o, alternativamente, se especifiquen los requisitos que se acaban de indicar.

Referencias de Interés

- Agencia Española de Protección de Datos: http://www.agpd.es/
- Agencia de Protección de Datos de la Comunidad de Madrid: http://www.apdcm.es/
- Agencia de Protección de Datos de la Comunidad de Catalunya: http://www.apdcat.net/
- Agencia de Protección de Datos del País Vasco: http://www.avpd.euskadi.net/
- US Search: http://www.ussearch.com/
- Acuerdo "Safe *Harbor*": http://www.export.gov/safeharbor/
- HIPPA (Estados Unidos): http://www.hhs.gov/ocr/hipaa/
- Página de información sobre Privacidad de la *Federal Trade Commission* (FTC): http://www.ftc.gov/privacy/
- OCDE: http://www.oecd.org/sti/security-privacy

ANEXO I Ley Orgánica de Protección de los Datos de Carácter Personal (LOPD, 15/1999)

TÍTULO I: DISPOSICIONES GENERALES

Artículo 1. Objeto.

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

Artículo 2. Ámbito de aplicación.

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.
   Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:
   a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
   b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
   c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.
2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:
   a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
   b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
   c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.
3 Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:
   a) Los ficheros regulados por la legislación de régimen electoral.
   b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
   c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
   d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
   e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. Definiciones.

A los efectos de la presente Ley Orgánica se entenderá por:
a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.
b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

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

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

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

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

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

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

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II: PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Artículo 4. Calidad de los datos.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

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

   Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.
6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

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

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

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

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.
5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.
Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. Consentimiento del afectado.

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. Datos especialmente protegidos.

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.
Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.
2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindi-

catos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.
6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

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

Artículo 8. Datos relativos a la salud.

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

Artículo 9. Seguridad de los datos.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber de secreto.

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

Artículo 11. Comunicación de datos.

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:
   a) Cuando la cesión está autorizada en una ley.
   b) Cuando se trate de datos recogidos de fuentes accesibles al público.
   c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

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

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

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

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.
4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.
5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.
6 Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

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

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
   En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III: DERECHOS DE LAS PERSONAS

Artículo 13. Impugnación de valoraciones.

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.
3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.
4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

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

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

Artículo 15. Derecho de acceso.

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.
3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.
   Cumplido el citado plazo deberá procederse a la supresión.
4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.
5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

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

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.
2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. Tutela de los derechos.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.
2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.
3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.
4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. Derecho a indemnización.

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

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.
3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV: DISPOSICIONES SECTORIALES

CAPÍTULO I: Ficheros de titularidad pública

Artículo 20. Creación, modificación o supresión.

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente.
2. Las disposiciones de creación o de modificación de ficheros deberán indicar:
   a) La finalidad del fichero y los usos previstos para el mismo.
   b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
   c) El procedimiento de recogida de los datos de carácter personal.
   d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
   e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
   f) Los órganos de las Administraciones responsables del fichero.
   g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
   h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.
3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. Comunicación de datos entre Administraciones públicas.

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.
3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.
4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

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

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.
2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.
3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.
   A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

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

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.
2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.
3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

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

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.
2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

CAPÍTULO II: Ficheros de titularidad privada

Artículo 25. Creación.

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

Artículo 26. Notificación e inscripción registral.

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.
2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.
3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.
   En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.
5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. Comunicación de la cesión de datos.

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.
2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

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

1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.
2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.
   Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.
   La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.
3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.
   En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.
4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

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

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.
2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.
3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.
4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

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

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.
2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.
3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.
4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. Censo promocional.

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.
2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.
3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento.

   Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.
4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. Códigos tipo.

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.
2. Los citados códigos podrán contener, o no, reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

   En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.
3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V: Movimiento internacional de datos.

Artículo 33. Norma general.

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.
2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación:

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

TÍTULO VI: Agencia de Protección de Datos.

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.
2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.
3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por fun-

cionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:
   a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.
   b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
   c) Cualesquiera otros que legalmente puedan serle atribuidos.
5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. El Director.

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

Artículo 37. Funciones.

Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.
d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.
e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.
f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.
g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.
h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.
i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.
k) Redactar una memoria anual y remitirla al Ministerio de Justicia.
l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.
m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.
n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 38. Consejo Consultivo.

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:
Un Diputado, propuesto por el Congreso de los Diputados.
Un Senador, propuesto por el Senado.
Un representante de la Administración Central, designado por el Gobierno.
Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.
Un miembro de la Real Academia de la Historia, propuesto por la misma.
Un experto en la materia, propuesto por el Consejo Superior de Universidades.
Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.
Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.
Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.
El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. El Registro General de Protección de Datos.

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.
2. Serán objeto de inscripción en el Registro General de Protección de Datos:
   a) Los ficheros de que sean titulares las Administraciones públicas.
   b) Los ficheros de titularidad privada.
   c) Las autorizaciones a que se refiere la presente Ley.
   d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
   e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.
3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. Potestad de inspección.

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.
   A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.
2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.
   Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. Órganos correspondientes de las Comunidades Autónomas.

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

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

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

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.
2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII: Infracciones y sanciones

Artículo 43. Responsables.

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.
2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. Tipos de infracciones.

1. Las infracciones se calificarán como leves, graves o muy graves.
2. Son infracciones leves:
   a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
   b)No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
   c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
   d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.
   e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.
3. Son infracciones graves:
   a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente.
   b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
   c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.
   d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
   e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
   f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

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

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

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

j) La obstrucción al ejercicio de la función inspectora.

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

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

4. Son infracciones muy graves:

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

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

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

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

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

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

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

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

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

Artículo 45. Tipo de sanciones.

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.
2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.
3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.
4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.
6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.
7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. Infracciones de las Administraciones públicas.

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción.
   Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.
2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran.
   El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.
3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.
4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. Prescripción.

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.
2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.
3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.
4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.
5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.
6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. Procedimiento sancionador.

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.
2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

Artículo 49. Potestad de inmovilización de ficheros.

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

Disposición adicional primera. Ficheros preexistentes.

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

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

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

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.
2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.

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

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

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

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

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

"4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado.

En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal."

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

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

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

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

"Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora.

La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos,

de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.
En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado."

Disposición transitoria primera. Tratamientos creados por Convenios internacionales.

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

Disposición transitoria segunda. Utilización del censo promocional.

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

Disposición transitoria tercera. Subsistencia de normas preexistentes.

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

Disposición derogatoria única. Derogación normativa.

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

Disposición final primera. Habilitación para el desarrollo reglamentario.

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

Disposición final segunda. Preceptos con carácter de Ley ordinaria.

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

Disposición final tercera. Entrada en vigor.

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

Por tanto,

Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta Ley Orgánica.
Madrid, 13 de diciembre de 1999.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ MARÍA AZNAR LÓPEZ

ANEXO II Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter Personal

(real decreto 994/1999, de 11 de junio de 1999)

CAPÍTULO I.- DISPOSICIONES GENERALES

Artículo 1.- Ámbito de aplicación y fines.

El presente Reglamento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal.

Artículo 2.- Definiciones.

A efectos de este Reglamento, se entenderá por:

1. Sistema de información: Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
2. Usuario: Sujeto o proceso autorizado para acceder a datos o recursos.
3. Recurso: Cualquier parte componente de un sistema de información.
4. Accesos autorizados: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.
5. Identificación: Procedimiento de reconocimiento de la identidad de un usuario.
6. Autenticación: Procedimiento de comprobación de la identidad de un usuario.
7 Control del acceso: Mecanismo que en función a la identificación ya autenticada permite acceder a datos o recursos.
8. Contraseña: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.
9. Incidencia: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
10. Soporte: Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.
11. 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.
12. Copia de respaldo: Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Artículo 3.- 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, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Artículo 4.- Aplicación de los niveles de seguridad.

1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.
2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el articulo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.
3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.
5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

Artículo 5.- 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 deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Artículo 6.- Régimen de trabajo fuera de los locales de la ubicación del fichero.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Artículo 7.- Ficheros temporales.

1. Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Reglamento.
2. Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II.- MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 8.- Documento de seguridad.

1. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.
2. 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.
   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.
3. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
4. El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Artículo 9.- Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas, de acuerdo con lo previsto en el artículo 8.2.c)
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 10.- Registro de incidencias.

El procedimiento de notificación y gestión de incidencias contendrá necesariamente 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 y los efectos que se hubieran derivado de la misma.

Artículo 11.- Identificación y autenticación.

1. El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.
2.- 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.
3. Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Artículo 12.- Control de acceso.

1. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
3. La relación de usuarios a la que se refiere el artículo 11.1 de este Reglamento contendrá el acceso autorizado para cada uno de ellos.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

Artículo 13.- Gestión de soportes.

1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.
2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

Artículo 14. - Copias de respaldo y recuperación.

1. El responsable de fichero se encargará de verificar la definición y correcta 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 deberán 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 periodo no se hubiera producido ninguna actualización de los datos.

CAPÍTULO III.- MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 15.- Documento de seguridad.

El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del presente Reglamento, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

Artículo 16.- Responsable de seguridad.

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

Artículo 17.- Auditoría.

1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.
2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, 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 recomendaciones propuestas.
3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Artículo 18.- Identificación y autenticación.

1. El responsable del fichero 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 verificación de que está autorizado.
2. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 19.- 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 20.- Gestión de soportes.

1. Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, 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 que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.
3. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.
4. Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Artículo 21.- Registro de incidencias.

1. En el registro regulado en el artículo 10 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 por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Artículo 22.- 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 tipo de fichero tratado.

CAPÍTULO IV.- MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 23.- Distribución de soportes.

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

Artículo 24.- 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 los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso, la desactivación 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.

Artículo 25.- Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

Artículo 26.- Telecomunicaciones.

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

CAPÍTULO V.- INFRACCIONES Y SANCIONES.

Artículo 27.- Infracciones y sanciones.

1. El incumplimiento de las medidas de seguridad descritas en el presente Reglamento será sancionado de acuerdo con lo establecido en los artículos 43 y 44 de la Ley Orgánica 5/1992, cuando se trate de ficheros de titularidad privada.
   El procedimiento a seguir para la imposición de la sanción a la que se refiere el párrafo anterior será el establecido en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.
2. Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 45 de la Ley Orgánica 5/1992.

Artículo 28.- Responsables.

Los responsables de los ficheros, sujetos al régimen sancionador de la Ley Orgánica 5/1992, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal en los términos establecidos en el presente Reglamento.

CAPÍTULO VI.- COMPETENCIAS DEL DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

Artículo 29.- Competencias del Director de la Agencia de Protección de Datos.

El Director de la Agencia de Protección de Datos podrá, de conformidad con lo establecido en el artículo 36 de la Ley Orgánica 5/1992:

1. Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos

automatizados a los principios de la Ley Orgánica 5/1992.

2. Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se cumplan las medidas de seguridad previstas en el presente Reglamento.

Disposición transitoria única.- Plazos de implantación de las medidas.

En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Reglamento, las medidas de seguridad de nivel básico previstas en el presente Reglamento deberán implantarse en el plazo de seis meses desde su entrada en vigor, las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años.

Cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento, la adecuación de dichos sistemas y la implantación de las medidas de seguridad deberán realizarse en el plazo máximo de tres años a contar desde la entrada en vigor del presente Reglamento.

ANEXO III Cuadro Resumen Medidas de Seguridad

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CUADRO RESUMEN MEDIDAS DE SEGURIDAD

Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal (RD 994/1999)

Nivel básico: Ficheros que contengan datos de carácter personal.
Nivel medio: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).
Nivel alto: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los recabados para fines policiales sin consentimiento de las personas afectadas.

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
DOCUMENTO DE SEGURIDAD	- Ambito de aplicación. - Medidas, normas, procedimientos reglas y estándares de seguridad. - Funciones y obligaciones del personal. - Estructura y descripción de ficheros y sistemas de información. - Procedimiento de notificación, gestión y respuesta ante incidencias. - Proced. realización copias de respaldo y recuperación de datos.	- Identificación del responsable de seguridad. - Control periódico del cumplimiento del documento. - Medidas a adoptar en caso de reutilización o desecho de soportes.	
PERSONAL	- Funciones y obligaciones claramente definidas y documentadas. - Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento.		
INCIDENCIAS	- Registrar tipo de incidencia, momento en que se ha producido, persona que la notificia, persona a la que se comunica y efectos derivados.	- Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente. - Autorización por escrito del responsable del fichero para su recuperación.	
IDENTIFICACIÓN Y AUTENTICACIÓN	- Relación actualizada de usuarios y accesos autorizados. - Procedimientos de identificación y autenticación. - Criterios de accesos. - Procedimientos de asignación y gestión de contraseñas y periodicidad con que se cambian. - Almacenamiento ininteligible de contraseñas activas.	- Se establecerá el mecanismos que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado. - Limite de intentos reiterados de acceso no autorizado.	
CONTROL DE ACCESO	- Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones. - Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. - Concesión de permisos de acceso sólo por personal autorizado.	- Control de acceso físico a los locales donde se encuenetren ubicados los sistemas de información.	
GESTIÓN DE SOPORTES	- Identificar el tipo de información que contienen. - Inventario. - Almacenamiento con acceso restringido. - Salida de soportes autorizada por el responsable del fichero.	- Registro de entrada y salida de soportes. - Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. - Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento.	- Cifrado de datos en la distribución de soportes.
COPIAS DE RESPALDO	- Verificar la definición y aplicación de los procedimientos de copias y recuperación. - Garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción. - Copia de respaldo, al menos semanal.		- Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
RESPONSABLE		- Uno o varios nombrados por el responsable del fichero. - Encargado de coordinar y controlar las medidas del documento. - No supone delegación de responsabilidad del responsable del fichero.	
PRUEBAS		- Solo se realizarán si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado.	
AUDITORIA		- Bianual, interna o externa. - Adecuación de las medidas y controles. - Deficiencias y propuestas correctoras. - Análisis del responsable de seguridad y conclusiones al responsable del fichero, - Adopción de las medidas correctoras adecuadas.	
REGISTRO DE ACCESOS			- Registrar usuario, hora, fichero, tipo acceso y registro accedido. - Control del responsable de seguridad. Informe mensual. - Conservación 2 años.
TELECOMUNICACIONES			- Transmisión de datos cifrada.

- Los niveles son acumulativos y tienen la condición de mínimos exigibles.
- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.
- La ejecución de trabajos fuera de los locales de la ubicación del fichero debe ser expresamente autorizada por el responsable del fichero y garantizar el nivel de seguridad.
- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.
- Los ficheros de nivel básico que contengan datos que permitan obtener una evaluación de la personalidad del individuo deberan garantizar, además de las medidas de nivel básico, las de nivel medio relativas a auditoria, identificación y autenticación, control de acceso físico y gestión de soportes.

ANEXO IV Contrato de Tratamiento de Datos

CONTRATO DE TRATAMIENTO DE DATOS ENTRE LA ENTIDAD ..... Y LA EMPRESA .....

Ciudad, fecha del contrato

POR UNA PARTE,

D. ....., en representación de la Entidad .....

POR OTRA PARTE,

D. ....., con DNI ....., en su calidad de Gerente, actuando en nombre y representación de la empresa ....., con domicilio social en .....

Las partes se reconocen mutuamente la capacidad legal suficiente para suscribir este contrato y quedar obligadas en la representación en que respectivamente actúan. Para tal fin, se establecen las siguientes

CONDICIONES GENERALES

1ª.- Que, como consecuencia de la prestación de servicios realizada por parte de la empresa ..... a la Entidad ....., la empresa ..... actúa como un encargado del tratamiento de datos en los términos previstos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
Para la realización de estos servicios es imprescindible y necesario que el encargado del tratamiento tenga acceso a la información contenida en los ficheros con datos de carácter personal de titularidad pública, de los cuales es responsable la Entidad .....

2ª.- El encargado del tratamiento tratará los datos de carácter personal de acuerdo con las instrucciones del responsable del fichero y solamente con las finalidades y los usos exclusivamente necesarios para el desarrollo de la actividad de prestación de servicios que le fue encomendada por el responsable del fichero, no pudiendo usarlos para un fin distinto.

3ª.- Los datos personales a los que tenga acceso el encargado del tratamiento no podrán ser comunicados a terceros ni siquiera para su conservación.

4ª.- El encargado del tratamiento se compromete a adoptar las medidas de índole técnico y organizativo que fuesen necesarias para garantizar la seguridad de los datos de carácter personal a los que tenga acceso y eviten su alteración, pérdida, tratamiento o acceso no autorizado. En cualquier caso ambas partes se comprometen a cumplir las medidas de seguridad, en función de los datos que vayan ser tratados, establecidas en el Real Decreto 994/1999.

6ª.- El encargado del tratamiento será obligado al secreto profesional con relación a los datos de carácter personal objeto del tratamiento, debiendo guardar secreto durante el tratamiento y con posterioridad a su finalización respondiendo frente al responsable del fichero, en el caso de incumplimiento sin perjuicio de las responsabilidades que se pudieran derivar ante la Agencia Española de Protección de Datos o directamente a los interesados.

7ª.- El encargado del tratamiento se compromete a comunicar y hacer cumplir a sus empleados, incluidos los trabajadores de empresas de trabajo temporal, las obligaciones establecidas en los apartados anteriores y, en concreto, las relativas al deber de secreto y medidas de seguridad, respondiendo frente al responsable del fichero, en el caso de incumplimiento sin perjuicio de las responsabilidades que se puedan derivar ante la Agencia Española de Protección de Datos o directamente del interesado.

8ª.- El encargado del tratamiento responderá directamente ante la Agencia Española de Protección de Datos de los incumplimientos que se pudiesen derivar de las condiciones anteriores.

ANEXO V Modelo de Inscripción de Ficheros de Titularidad Pública

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PÚBLICA

Tipo de Solicitud

- ☐ Inscripción de creación de fichero
- ☐ Inscripción de modificación de fichero
- ☐ Inscripción de supresión de fichero

(A consignar en la Agencia de Protección de Datos)

Fecha de entrada:

Número de Registro:

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el abajo firmante en su calidad de *indíquese la relación con el responsable, especificando el puesto desempeñado, o en su caso, representante* de *indíquese la denominación completa de la Entidad u Organismo responsable del fichero declarado* con CIF *indíquese el CIF del responsable* , con representación suficiente, formula la siguiente notificación, y manifiesta que todos los datos consignados son ciertos.

PERSONA FÍSICA QUE EFECTÚA LA NOTIFICACIÓN

Nombre | Primer Apellido | Segundo Apellido

DIRECCIÓN A EFECTOS DE NOTIFICACIÓN

Tipo Vía | Nombre de Vía | Número | Piso, Pta, Esc.

Localidad | Código Postal

Provincia | País

Teléfono | Fax | E-mail

En _____ a ____ de _____ de _____

Fdo.:

En cumplimiento del artículo 5 de la Ley 15/1999, por el que se regula el derecho de información en la recogida de los datos, se advierte de los siguientes extremos: Los datos de carácter personal, que pudieran constar en esta notificación, se incluirán en el fichero de nombre *"Registro General Protección de Datos"*, creado por Resolución del Director de la Agencia de fecha 18 de junio de 1994, (B.O.E. nº 180, 29-7-94), por la que se regulan los ficheros automatizados de datos de carácter personal existentes en la Agencia de Protección de Datos. La finalidad del fichero es velar por la publicidad de la existencia de los ficheros que contengan datos de carácter personal con el fin de hacer posible el ejercicio de los derechos de información, oposición, acceso, rectificación y cancelación de los datos. Los datos relativos a la persona física que actúa como declarante de la notificación, únicamente se utilizarán en los términos previstos en los procedimientos administrativos que sean necesarios para la tramitación de la correspondiente solicitud. Tendrá derecho a acceder a sus datos personales informatizados, rectificarlos o en su caso cancelarlos en la Agencia de Protección de Datos, órgano responsable del fichero.

En caso de que en la notificación deban incluirse datos de carácter personal, referentes a personas físicas distintas de la que efectúa la solicitud o del responsable del fichero, deberá, con carácter previo a su inclusión, informarles de los extremos contenidos en el párrafo anterior.

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 1

LEY ORGANICA 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal. Su finalidad es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

RESPONSABLE DEL FICHERO O TRATAMIENTO

1. Responsable del Fichero o Tratamiento. (Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento)

Administración a la que pertenece

- ❑ Administración General del Estado, Organismos Públicos del Estado y Organismos de la Seguridad Social
- ❑ Administración y Organismos Públicos de Comunidades Autónomas — Comunidad Autónoma
- ❑ Administración y Organismos Públicos de Entidades Locales
- ❑ Otras Personas Jurídico-Públicas

Encuadramiento administrativo del órgano:

Ministerio/Consejería/Entidad Local

Dirección General./Dependencia Municipal / Organismo Público

Nombre del órgano administrativo

CIF

Dirección

Tipo Vía | Nombre de Vía | Número | Piso, Pta, Esc.

Localidad | Código Postal

Provincia | País

Teléfono | Fax | E-mail

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 2

OPOSICION ACCESO RECTIFICACION Y CANCELACION

2. Servicio o Unidad concreto ante el que puedan ejercitarse los derechos de oposición, acceso, rectificación y cancelación. (Cumplimentar en el caso de que sea diferente al declarado en el apartado 1. *Responsable del Fichero o Tratamiento*)

Nombre de la Oficina o Dependencia

Dirección

Tipo Vía | Nombre de Vía | Número | Piso, Pta, Esc.

Localidad | Código Postal

Provincia | País

Teléfono | Fax | E-mail

DISPOSICION GENERAL

3. Disposición general de creación, modificación o supresión del fichero. (Disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente, relativa a la creación, modificación o supresión de los ficheros de las Administraciones Públicas)

Diario Oficial de Publicación

☐ BOLETÍN OFICIAL DEL ESTADO
☐ BOLETÍN DE COMUNIDADES AUTÓNOMAS
☐ OTROS

Número de Boletín | Fecha

Disposición General de | Creación ☐ | Modificación ☐ | Supresión ☐

Indicar la Disposición General

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 3

NOMBRE DEL FICHERO O TRATAMIENTO

4. Nombre y descripción del fichero o tratamiento de datos. (Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias)

Nombre del fichero o tratamiento de datos

Descripción

ENCARGADO DEL TRATAMIENTO

5. Encargado del tratamiento.(La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero o tratamiento). Cumplimentar únicamente cuando un tercero realiza el tratamiento por cuenta del responsable

❑ Persona física o Entidad Privada Código Actividad Principal

Nombre de la Oficina o Dependencia
(En caso de Persona física o Entidad Privada indicar nombre o Razón Social)

NIF/CIF

Dirección

Tipo Vía Nombre de Vía Número Piso, Pta, Esc.

Localidad Código Postal

Provincia País

Teléfono Fax E-mail

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 4

MEDIDAS DE SEGURIDAD

6. Medidas de seguridad.

Las medidas de seguridad adoptadas son de nivel

☐ Básico ☐ Medio ☐ Alto

ESTRUCTURA BASICA

7. Estructura básica y descripción de los tipos de datos de carácter personal incluidos en el fichero.

Datos especialmente protegidos

☐ IDEOLOGÍA
☐ AFILIACIÓN SINDICAL
☐ RELIGIÓN
☐ CREENCIAS

¿Han sido recabados con consentimiento expreso y por escrito del afectado?
☐ SÍ ☐ NO

¿Es un fichero mantenido por 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, siempre que se refiera a sus asociados o miembros?

☐ SÍ ☐ NO

Otros datos especialmente protegidos

☐ ORIGEN RACIAL O ÉTNICO
☐ SALUD
☐ VIDA SEXUAL

¿Han sido recabados con consentimiento expreso del afectado?
☐ SÍ ☐ NO

¿Existe una Ley que permite su recogida, tratamiento y cesión, por razones de interés general?
☐ SÍ ☐ NO

Si ha contestado SÍ a la pregunta anterior, especifique la Ley que exime del consentimiento expreso por razones de interés general

Indicar la Ley referida **Nº Ley** **Año**

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PÚBLICA

C.I.F. DEL TITULAR ☐

Página: 5

ESTRUCTURA BASICA

Datos relativos a la comisión de infracciones penales o administrativas

☐ INFRACCIONES PENALES
☐ INFRACCIONES ADMINISTRATIVAS

Indique la norma reguladora que le habilita al responsable a incluir estos datos en el fichero.

Nº ☐ **Año** ☐

Datos de carácter identificativo

☐ D.N.I./N.I.F.
☐ Nº S.S./MUTUALIDAD
☐ NOMBRE Y APELLIDOS
☐ DIRECCIÓN (POSTAL, ELECTRÓNICA)
☐ TELÉFONO
☐ OTROS (indicar)
☐ FIRMA/HUELLA DIGITALIZADA
☐ IMAGEN/VOZ
☐ MARCAS FÍSICAS
☐ Nº REGISTRO PERSONAL
☐ FIRMA ELECTRÓNICA

Datos de características personales

☐ DATOS DE ESTADO CIVIL
☐ DATOS DE FAMILIA
☐ FECHA DE NACIMIENTO
☐ LUGAR DE NACIMIENTO
☐ EDAD
☐ OTROS (indicar)
☐ SEXO
☐ NACIONALIDAD
☐ LENGUA MATERNA
☐ CARACTERÍSTICAS FÍSICAS O ANTROPOMÉTRICAS

Datos de circunstancias sociales

☐ CARACTERÍSTICAS DE ALOJAMIENTO, VIVIENDA
☐ SITUACIÓN MILITAR
☐ PROPIEDADES, POSESIONES
☐ AFICIONES Y ESTILOS DE VIDA
☐ PERTENENCIA A CLUBES, ASOCIACIONES
☐ LICENCIAS, PERMISOS, AUTORIZACIONES
☐ OTROS (indicar)

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 6

ESTRUCTURA BASICA

Datos académicos y profesionales

- ☐ FORMACIÓN, TITULACIONES
- ☐ HISTORIAL DE ESTUDIANTE
- ☐ EXPERIENCIA PROFESIONAL
- ☐ PERTENENCIA A COLEGIOS O A ASOCIACIONES PROFESIONALES
- ☐ OTROS (indicar)

Datos de detalles de empleo

- ☐ CUERPO / ESCALA
- ☐ CATEGORÍA / GRADO
- ☐ PUESTOS DE TRABAJO
- ☐ DATOS NO ECONÓMICOS DE NÓMINA
- ☐ HISTORIAL DEL TRABAJADOR
- ☐ OTROS (indicar)

Datos de información comercial

- ☐ ACTIVIDADES Y NEGOCIOS
- ☐ LICENCIAS COMERCIALES
- ☐ SUSCRIPCIONES A PUBLICACIONES/MEDIOS DE COMUNICACIÓN
- ☐ CREACIONES ARTÍSTICAS, LITERARIAS, CIENTÍFICAS O TÉCNICAS
- ☐ OTROS (indicar)

Datos económico-financieros y de seguros

- ☐ INGRESOS, RENTAS
- ☐ INVERSIONES, BIENES PATRIMONIALES
- ☐ CRÉDITOS, PRÉSTAMOS, AVALES
- ☐ DATOS BANCARIOS
- ☐ PLANES DE PENSIONES, JUBILACIÓN
- ☐ DATOS ECONÓMICOS DE NÓMINA
- ☐ DATOS DEDUCCIONES IMPOSITIVAS/IMPUESTOS
- ☐ SEGUROS
- ☐ HIPOTECAS
- ☐ SUBSIDIOS, BENEFICIOS
- ☐ HISTORIAL CRÉDITOS
- ☐ TARJETAS CRÉDITO
- ☐ OTROS (indicar)

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 7

ESTRUCTURA BASICA

Datos de transacciones

- ☐ BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO
- ☐ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO
- ☐ TRANSACCIONES FINANCIERAS
- ☐ COMPENSACIONES / INDEMNIZACIONES
- ☐ OTROS (indicar)

FINALIDAD DEL FICHERO Y USOS PREVISTOS

8. Finalidad del fichero y usos previstos.

8.a) Descripción detallada de la finalidad y usos previstos

8.b) Tipificación correspondiente a la finalidad y usos previstos

RECURSOS HUMANOS

- q GESTIÓN DE PERSONAL
- q GESTIÓN DE NÓMINA
- q FORMACIÓN DE PERSONAL
- q ACCIÓN SOCIAL A FAVOR DEL PERSONAL DE LAS ADMINISTRACIONES PÚBLICAS
- q PROMOCIÓN Y SELECCIÓN DE PERSONAL, OPOSICIONES Y CONCURSOS
- q PREVENCIÓN DE RIESGOS LABORALES
- q CONTROL HORARIO
- q CONTROL DE INCOMPATIBILIDADES
- q CONTROL DE PATRIMONIO DE ALTOS CARGOS

HACIENDA Y GESTIÓN ECONOMICO-FINANCIERA

- q GESTIÓN TRIBUTARIA Y DE RECAUDACIÓN
- q GESTIÓN ECONÓMICA Y CONTABLE
- q GESTIÓN DE FACTURACIÓN
- q GESTIÓN FISCAL
- q GESTIÓN DEUDA PÚBLICA Y TESORERÍA
- q GESTIÓN DE CATASTROS INMOBILIARIOS RÚSTICOS Y URBANOS
- q RELACIONES COMERCIALES CON EL EXTERIOR
- q REGULACIÓN DE MERCADOS FINANCIEROS
- q DEFENSA DE LA COMPETENCIA

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 8

FINALIDAD DEL FICHERO Y USOS PREVISTOS

JUSTICIA

- q PROCEDIMIENTOS JUDICIALES
- q REGISTROS VINCULADOS CON LA FÉ PÚBLICA
- q PRESTACIÓN SOCIAL SUSTITUTORIA
- q TRAMITACIÓN DE INDULTOS

SEGURIDAD PUBLICA Y DEFENSA

- q PROTECCIÓN CIVIL
- q SEGURIDAD VIAL
- q ACTUACIONES DE FUERZAS Y CUERPOS DE SEGURIDAD CON FINES POLICIALES
- q ACTUACIONES DE FUERZAS Y CUERPOS DE SEGURIDAD CON FINES ADMINISTRATIVOS
- q GESTIÓN Y CONTROL DE CENTROS E INSTITUCIONES PENITENCIARIAS
- q TRAMITACIÓN DEL SERVICIO MILITAR
- q SOLICITUDES DE VISADO/RESIDENCIA

TRABAJO Y BIENESTAR SOCIAL

- q PROMOCIÓN Y GESTIÓN DE EMPLEO
- q RELACIONES LABORALES Y CONDICIONES DE TRABAJO
- q INSPECCIÓN Y CONTROL DE SEGURIDAD Y PROTECCIÓN SOCIAL
- q FORMACIÓN PROFESIONAL OCUPACIONAL
- q PRESTACIONES A DESEMPLEADOS
- q PRESTACIONES DE GARANTÍA SALARIAL
- q PRESTACIONES DE ASISTENCIA SOCIAL
- q PENSIONES, SUBSIDIOS Y OTRAS PRESTACIONES ECONÓMICAS
- q ACCIÓN A FAVOR DE INMIGRANTES
- q SERVICIOS SOCIALES A MINUSVÁLIDOS
- q SERVICIOS SOCIALES A LA TERCERA EDAD
- q PROMOCIÓN SOCIAL A LA MUJER
- q PROMOCIÓN SOCIAL A LA JUVENTUD
- q PROTECCIÓN DEL MENOR
- q ACCIÓN A FAVOR DE TOXICÓMANOS
- q AYUDAS ACCESO A VIVIENDA
- q OTROS SERVICIOS SOCIALES

SANIDAD

- q GESTIÓN Y CONTROL SANITARIO
- q HISTORIAL CLÍNICO
- q INVESTIGACIÓN EPIDEMIOLÓGICA Y ACTIVIDADES ANÁLOGAS
- q GESTIÓN DE TARJETA SANITARIA

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 9

FINALIDAD DEL FICHERO Y USOS PREVISTOS

EDUCACION Y CULTURA

- q ENSEÑANZA INFANTIL Y PRIMARIA
- q ENSEÑANZA SECUNDARIA
- q ENSEÑANZA SUPERIOR
- q ENSEÑANZAS ARTÍSTICAS E IDIOMAS
- q EDUCACIÓN ESPECIAL
- q BECAS Y AYUDAS A ESTUDIANTES
- q DEPORTES
- q FOMENTO Y APOYO A ACTIVIDADES ARTÍSTICAS Y CULTURALES
- q PROTECCIÓN DEL PATRIMONIO HISTÓRICO-ARTÍSTICO

ESTADISTICA

- q FUNCIÓN ESTADÍSTICA PÚBLICA
- q PADRÓN DE HABITANTES
- q GESTIÓN DEL CENSO PROMOCIONAL
- q ENCUESTAS SOCIOLÓGICAS Y DE OPINIÓN

FINALIDADES VARIAS

- q PROCEDIMIENTOS ADMINISTRATIVOS
- q REGISTRO DE ENTRADA Y SALIDA DE DOCUMENTOS
- q OTROS REGISTROS ADMINISTRATIVOS
- q ATENCIÓN AL CIUDADANO
- q CONCESIÓN Y GESTIÓN DE PERMISOS, LICENCIAS Y AUTORIZACIONES
- q SEGURIDAD Y CONTROL DE ACCESO A EDIFICIOS
- q PUBLICACIONES
- q FINES CIENTÍFICOS, HISTÓRICOS O ESTADÍSTICOS
- q GESTIÓN SANCIONADORA
- q GESTIÓN DE ESTADÍSTICAS INTERNAS
- q PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN
- q OTRAS FINALIDADES

PERSONAS O COLECTIVOS

9.- Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 10

PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA

10. Procedencia y procedimiento de recogida de los datos

10.a) Procedencia de los datos

- ☐ EL PROPIO INTERESADO O SU REPRESENTANTE LEGAL
- ☐ OTRAS PERSONAS FÍSICAS DISTINTAS DEL AFECTADO O SU REPRESENTANTE
- ☐ FUENTES ACCESIBLES AL PÚBLICO
  - ☐ CENSO PROMOCIONAL
  - ☐ GUIAS DE SERVICIOS DE TELECOMUNICACIONES
  - ☐ LISTAS DE PERSONAS PERTENECIENTES A GRUPOS PROFESIONALES
  - ☐ DIARIOS Y BOLETINES OFICIALES
  - ☐ MEDIOS DE COMUNICACIÓN
- ☐ REGISTROS PÚBLICOS
- ☐ ENTIDAD PRIVADA
- ☐ ADMINISTRACIONES PÚBLICAS

10.b) Procedimiento de recogida

- ☐ ENCUESTAS O ENTREVISTAS
- ☐ FORMULARIOS O CUPONES
- ☐ TRANSMISIÓN ELECTRÓNICA DE DATOS / INTERNET
- ☐ OTROS (Indicar)

10.c) Soporte utilizado para la obtención

- ☐ SOPORTE PAPEL
- ☐ SOPORTE INFORMÁTICO / MAGNÉTICO
- ☐ VIA TELEMÁTICA
- ☐ OTROS (Indicar)

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 11

CESIONES O COMUNICACIONES DE DATOS

11. Cesión o comunicación de datos. (Se entiende por cesión o comunicación de datos toda revelación de datos realizada a una persona distinta del interesado)
Cumplimentar en el caso de que esté prevista una cesión o comunicación de datos

11.a) Supuestos en los que se ampara la cesión o la comunicación de los datos

¿Existe consentimiento de los afectados?	☐ SÍ ☐ NO
¿Existe una norma reguladora que las autoriza?	☐ SÍ ☐ NO
En caso afirmativo, indicar la norma reguladora Número Año	
¿El tratamiento responde a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la comunicación de los datos a terceros?	☐ SÍ ☐ NO
¿Corresponden a competencias idénticas o que versan sobre las mismas materias, ejercidas por otras Administraciones Públicas?	☐ SÍ ☐ NO
¿La comunicación tiene por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos?	☐ SÍ ☐ NO
¿Son datos obtenidos o elaborados con destino a otra Administración Pública?	☐ SÍ ☐ NO
¿Se trata de datos recogidos de fuentes accesibles al público?	☐ SÍ ☐ NO

11.b) Destinatarios de la cesión o comunicación

NIF/CIF	Nombre, Razón Social u Organismo

Otros destinatarios determinados

En caso de destinatarios determinables o categorías de destinatarios, indicar las reglas que permiten su identificación

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 12

TRANSFERENCIAS INTERNACIONALES S

12. Transferencias internacionales de datos

12.a) Supuestos legales que habilitan la realización de la transferencia internacional de datos: (Si la transferencia internacional de datos no se encuentra amparada por ninguno de los siguientes supuestos, deberá proceder a solicitar la correspondiente autorización del Director de la Agencia de Protección de Datos)

¿Se efectúa con destino a países que proporcionan un nivel de protección equiparable?	SÍ	NO
¿Resulta de la aplicación de tratados o convenios en los que sea parte España?	SÍ	NO
¿Se realiza a efectos de prestar o solicitar auxilio judicial internacional?	SÍ	NO
¿Es necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios?	SÍ	NO
¿Se refiere a transferencias dinerarias, conforme a su legislación específica?	SÍ	NO
¿El afectado ha dado su consentimiento?	SÍ	NO
¿Es 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?	SÍ	NO
¿Es 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?	SÍ	NO
¿Es necesaria o legalmente exigida para la salvaguarda de un interés público?	SÍ	NO
¿Es precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial?	SÍ	NO
¿Se efectúa, a petición de persona con interés legítimo, desde un Registro Público y es acorde con la finalidad del mismo?	SÍ	NO

12.b) Destinatarios de la transferencia

País	Nombre o Razón Social

Otros destinatarios determinados

En caso de destinatarios determinables o categorías de destinatarios, indicar las reglas que permiten su identificación

AGENCIA DE PROTECCION DE DATOS

MODELO DE NOTIFICACIÓN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS DE TITULARIDAD PUBLICA

C.I.F. DEL TITULAR

Página: 13

SUPRESIÓN

13. Supresión de la inscripción del fichero

Código de inscripción asignado por la Agencia

Motivos de la supresión

Destino de la información o previsiones adoptadas para su destrucción

MODIFICACIÓN

14.- Modificación de fichero

Código de inscripción asignado por la Agencia

Apartados a modificar

- ☐ Responsable del fichero o tratamiento
- ☐ Servicio o unidad dónde ejercitar los derechos de oposición, acceso, rectificación y cancelación
- ☐ Disposición de creación, modificación o supresión del fichero
- ☐ Nombre y descripción del fichero o tratamiento de datos
- ☐ Encargado del tratamiento
- ☐ Medidas de seguridad
- ☐ Estructura básica y descripción de los tipos de datos
- ☐ Finalidad del fichero y usos previstos
- ☐ Personas o colectivos afectados
- ☐ Procedencia y procedimiento de recogida de los datos
- ☐ Cesión o comunicación de datos
- ☐ Transferencias internacionales de datos

ANEXO VI Modelos de Documentos que Pueden utilizar los Ciudadanos para Ejercer sus Derechos en Relación con los Datos de Carácter Personal

A. EJERCICIO DEL DERECHO DE ACCESO

Petición de información sobre los datos personales incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:.....
Dirección de la Oficina de Acceso: C/.....
nº.....C.P.....Localidad:.....Provincia:.....

DATOS DEL SOLICITANTE

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia ..... C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con los artículos 15 de la Ley Orgánica 15/1999, y los artículos 12 y 13 del Real Decreto 1332/94.

SOLICITA.

1. Que se le facilite gratuitamente el acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada. En este caso se interpondrá la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de derechos, en virtud del artículo 18 de la Ley Orgánica y 17 del Real Decreto.

2. Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.

3. Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona están incluidos en sus ficheros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En ..... a ..... de ..... de 200 .....

B. EJERCICIO DE LOS DERECHOS DE RECTIFICACIÓN

Petición de corrección de datos personales inexactos o incorrectos objeto de tratamiento incluidos en un fichero

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:.....
Dirección de la Oficina de Acceso: C/..... nº..... C.P.....
Localidad:..... Provincia:.....

DATOS DEL SOLICITANTE

D/ Dª ....., mayor de edad, con domicilio en la calle ..... nº....., Localidad ....., Provincia ..... C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 15 y 16 del Real Decreto 1332/94.

SOLICITA.

1. Que se proceda gratuitamente a la efectiva corrección en el plazo de diez días desde la recepción de esta solicitud, de los datos inexactos relativos a mi persona que se encuentren en sus ficheros.

2. Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.

3. Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.

4. Que, en el caso de que el responsable del fichero considere que la rectificación o la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En ..... a ..... de ..... de 200 .....

ANEXO DATOS QUE DEBEN RECTIFICARSE

	Dato incorrecto	Dato correcto	Documento Acreditativo
1.	.....	.....	.....
2.	.....	.....	.....
3.	.....	.....	.....
4.	.....	.....	.....
5.	.....	.....	.....
6.	.....	.....	.....
7.	.....	.....	.....
8.	.....	.....	.....
9.	.....	.....	.....
10.	.....	.....	.....

C. EJERCICIO DEL DERECHO DE CANCELACIÓN

Petición de cancelación de datos personales objeto de tratamiento incluido en un fichero

DATOS DEL RESPONSABLE DEL FICHERO

Nombre:.....
Dirección de la Oficina de Acceso : C/..... nº..... C.P. .....
Localidad .....Provincia:.....

DATOS DEL SOLICITANTE

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia .....C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 15 y 16 del Real Decreto 1332/94.

SOLICITA.

1. Que en el plazo de diez días desde la recepción de esta solicitud, se proceda a la efectiva cancelación de cualesquiera datos relativos a mi persona que se encuentren en sus ficheros, en los términos previstos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y me lo comuniquen de forma escrita a la dirección arriba indicada.

2. Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En ..... a ..... de ..... de 200 .....

E. DENUNCIA ANTE LA INSPECCIÓN DE LA AGENCIA DE PROTECCIÓN DE DATOS

1. DATOS DEL DENUNCIANTE

D..... con D.N.I. número....., del que acompaña fotocopia, actuando en su propio nombre y representación, con domicilio a efecto de notificaciones en ..... (localidad), C.P ..... Provincia ..... calle/avda/plaza .....

2. DATOS DEL DENUNCIADO

La Empresa/ el Organismo Público/Profesional/ Particular de nombre .... con CIF/NIF ....., y domicilio en calle/avda/plaza ..... Localidad ..... CP ..... Provincia .....

3. APORTA LA DOCUMENTACIÓN SIGUIENTE (enumerar):

1.
2.
3.
4.

4. DENUNCIA LOS HECHOS SIGUIENTES:

1.
2.
3.
4.

5. SOLICITA: Que al amparo de lo establecido en el artículo 48 de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal, interpone por medio del presente escrito denuncia por vulneración de lo dispuesto en dicha Ley.

En ..... a ..... de ..... de 200....

Firma (Adjuntar fotocopia del D.N.I.)

ILMO. SR. DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

F. RECLAMACIÓN ANTE LA INSPECCIÓN DE LA AGENCIA DE PROTECCIÓN DE DATOS POR DENEGACIÓN DEL DERECHO DE ACCESO

1. DATOS DEL RECLAMANTE

D./Dª. .....con D.N.I. número....., del que acompaña fotocopia, actuando en su propio nombre y representación, con domicilio a efecto de notificaciones en calle/avda/plaza..... Localidad..... C.P..... Provincia .....

2. DATOS DEL RESPONSABLE DEL FICHERO

La Empresa / el Organismo Público / Profesional / Particular, de nombre .... con CIF/NIF....., domicilio en calle/avda/plaza..... Localidad..... CP..... Provincia .....

3. APORTA LA DOCUMENTACIÓN SIGUIENTE (Márquese con una cruz):

- ☐ Copia de la carta remitida al responsable del fichero
- ☐ Copia de la contestación del responsable del fichero
- ☐ Otros (especificar)

4. RECLAMA POR DENEGACIÓN DEL EJERCICIO DEL DERECHO DE ACCESO (Márquese con una cruz):

- ☐ No se ha contestado en el plazo de un mes desde la recepción de la solicitud.
- ☐ Se ha denegado el acceso completamente.
- ☐ No se ha contestado satisfactoriamente a la petición de acceso.

5. SOLICITA: Que al amparo de lo establecido en el artículo 18 de la Ley Orgánica 15/1999, de proteccion de datos de carácter personal, interpone por medio del presente escrito reclamación por vulneración del artículo15 de la referida Ley Orgánica, y los artículos 12, 13 y 14 del Real Decreto 1332/1994 de desarrollo de esta Ley.

En ..... a ..... de ..... de 200 .... (Adjuntar fotocopia del D.N.I.)
Firma

ILMO. SR. DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

G. RECLAMACIÓN ANTE LA INSPECCIÓN DE LA AGENCIA DE PROTECCIÓN DE DATOS POR DENEGACIÓN DEL DERECHO DE RECTIFICACIÓN

1. DATOS DEL RECLAMANTE

D./Dª. ..... con D.N.I. número....., del que acompaña fotocopia, actuando en su propio nombre y representación, con domicilio a efecto de notificaciones en calle/avda/plaza..... Localidad..... C.P.....Provincia.....

2. DATOS DEL RESPONSABLE DEL FICHERO

La Empresa / el Organismo Público / Profesional / Particular, de nombre ....con CIF/NIF....., domicilio en calle/avda/plaza..... Localidad..... CP..... Provincia .....

3. APORTA LA DOCUMENTACIÓN SIGUIENTE (Márquese con una cruz):

- ☐ Fotocopia de la carta remitida al responsable del fichero
- ☐ Contestación por parte del responsable del fichero
- ☐ Otros (especificar)

4. RECLAMA POR DENEGACIÓN DEL EJERCICIO DEL DERECHO DE RECTIFICACIÓN (M. con una cruz):

- ☐ No se ha contestado en el plazo de diez días
- ☐ Se ha denegado la rectificación total o parcialmente sin justificación
- ☐ Se ha denegado la rectificación total o parcialmente razonadamente
- ☐ No se ha rectificado el dato de modo efectivo
- ☐ Otros (especificar)

5. SOLICITA: Que al amparo de lo establecido en el artículo 18 de la Ley Orgánica 15/1999, de protección de datos de carácter personal, interpone por medio del presente escrito reclamación por vulneración del artículo 16 de la referida Ley Orgánica y el artículo 15 del Real Decreto 1332/1994.

En ..... a ..... de ..... de 200 .... (Adjuntar fotocopia del D.N.I.)

Firma

ILMO. SR. DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

H. RECLAMACIÓN ANTE LA INSPECCIÓN DE LA AGENCIA DE PROTECCIÓN DE DATOS POR DENEGACIÓN DEL DERECHO DE CANCELACIÓN

1. DATOS DEL RECLAMANTE

D./Dª..... con D.N.I.. número....., del que acompaña fotocopia, actuando en su propio nombre y representación, con domicilio a efecto de notificaciones en calle/avda/plaza ..... Localidad..... C.P..... Provincia .....

2. DATOS DEL RESPONSABLE DEL FICHERO

La Empresa / el Organismo Público / Profesional / Particular, de nombre ....con CIF/NIF ....., domicilio en calle/avda/plaza..... Localidad ..... CP..... Provincia .....

3. APORTA LA DOCUMENTACIÓN SIGUIENTE (Márquese con una cruz):

- ☐ Copia de la carta remitida al responsable del fichero
- ☐ Copia de la contestación del responsable del fichero
- ☐ Otros (especificar)

4. RECLAMA POR DENEGACIÓN DEL EJERCICIO DEL DERECHO DE CANCELACIÓN (M. con una cruz):

- ☐ No se ha contestado en el plazo de diez días
- ☐ Se ha denegado la cancelación total o parcialmente sin justificación
- ☐ Se ha denegado la cancelación total o parcialmente razonadamente
- ☐ El responsable no ha procedido a la cancelación de los datos
- ☐ Otros (indicar)

5. SOLICITA: Que al amparo de lo establecido en el artículo 18 de la Ley Orgánica 15/1999, de proteccion de datos de datos de carácter personal, interpone por medio del presente escrito reclamación por vulneración del artículo16 de la referida Ley Orgánica y el artículo 15 del Real Decreto 1332/1994.

En ..... a ..... de ..... de 200 ..... (Adjuntar fotocopia del D.N.I.)
Firma

ILMO. SR. DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

ANEXO VII Modelo de Documento de Seguridad de la Deputación de Ourense

ÍNDICE

Ámbito de Aplicación del Documento de Seguridad

1.1. Ámbito Jurídico

Este Documento de Seguridad se ha elaborado para dar cumplimiento a la Ley Orgánica 15/99 de 13 de Diciembre de Protección de Datos de Carácter Personal, así como al Real Decreto 994/1999, de 11 de Junio por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal, y es de obligado cumplimiento para todo el personal de la Excma. DIPUTACIÓN PROVINCIAL DE OURENSE (En próximas referencias, Diputación).

El presente Documento de Seguridad se mantiene en todo momento actualizado y es revisado siempre que se producen cambios relevantes en los Sistemas de Información o en la organización del mismo.

Así pues, revisados los ficheros y archivos susceptibles de contener datos de carácter personal, se determina que el nivel de seguridad exigido en la Diputación es el NIVEL ALTO.

1.2. Ámbito Personal

Este Documento de Seguridad es de obligado cumplimiento para todo el personal de la Excma. DIPUTACIÓN PROVINCIAL DE OURENSE. Las normas internas contenidas en este documento se han puesto en conocimiento de todo el personal de la Entidad, con el objeto de dar debido cumplimiento a la Ley Orgánica 15/99, de 13 de Diciembre y al Real Decreto 994/1999, de 11 de Junio.

Todas las personas que tengan acceso a los datos de los ficheros de la Excma. DIPUTACIÓN PROVINCIAL DE OURENSE, bien a través del Sistema Informático habilitado para acceder al mismo, o bien a través de cualquier otro medio automatizado de acceso, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos del/de los ficheros, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

La estructura para la aplicación de la Política de Seguridad se establece como sigue:

Responsable de Ficheros: DIPUTACIÓN PROVINCIAL DE OURENSE

Responsable de Seguridad: El Jefe del servicio de Informática y Nuevas Tecnologías o, en su ausencia, el Técnico en Redes y Seguridad.

1.3. Ámbito Material

La protección de los datos de los ficheros frente a accesos no autorizados se deberá limitar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan:

CENTROS DE TRABAJO	UBICACIÓN
DIPUTACIÓN PROVINCIAL DE OURENSE	C/ Progreso Nº 32, Ourense

Asimismo, la Diputación posee un Sistema Informático constituido principalmente por un conjunto de servidores que gestionan toda la información a través de diversas aplicaciones a las cuales tienen acceso determinados equipos de la red. Los usuarios son sólo los empleados de esta administración.

En el apartado que viene a continuación (Sistemas Informáticos) se recogen las normas de seguridad que son de aplicación a los anteriores recursos informáticos de la Diputación.

SISTEMAS INFORMÁTICOS

2.1. Medidas de Seguridad en Sistemas Informáticos

2.1.1. Descripción general del Sistema

La estructura general del Sistema Informático de la Diputación se basa en una red corporativa formada por los sistemas que se describen en el **Anexo 3**.

2.1.2. Identificación y autenticación para el acceso a la Red Informática

El Responsable de Seguridad ha elaborado una relación actualizada de usuarios con acceso autorizado al sistema de información. Dicha relación se incluye en el Documento de Seguridad como **Anexo 2**.

El Responsable de Seguridad custodia y actualiza la relación de todos los usuarios de la red que tienen acceso autorizado al sistema de información.

Procedimiento de identificación y autenticación para el acceso a la red informática:

Se dispone de un sistema de identificación por contraseñas contrastadas con un servidor central.

Todos los usuarios del sistema tienen asignado un identificador y una contraseña. La contraseña tiene un número limitado mínimo de 6 caracteres alfanuméricos.

El sistema de autenticación se basa en un entorno de clave de conexión de redes contrastada contra un servidor con Windows 2000 Server.

El usuario introduce su identificador (que le identifica como usuario autorizado al acceso) y su contraseña (que le autentifica como el usuario identificado), que son verificados en el servidor, el cual le reconoce como usuario del sistema, permitiéndole acceder a los recursos de la red.

2.1.3. Procedimiento de asignación, distribución y almacenamiento de contraseñas para el acceso a la Red Informática

ASIGNACIÓN Y DISTRIBUCIÓN DE CONTRASEÑAS

Es competencia del Responsable de Seguridad, que la atribución y asignación de contraseñas, así como la custodia de la relación de usuarios, se realice de forma que se garantice su confidencialidad e integridad.

La asignación de contraseñas se realiza por el propio usuario, quien determina su propia contraseña de acceso al sistema.

La distribución de las contraseñas se realizará de manera que ni siquiera el usuario pueda visualizar la clave asociada a su identificador. Esta visualización se produce por la entrada del símbolo asterisco en pantalla cada vez que se introduce un carácter en la misma.

ALMACENAMIENTO DE CONTRASEÑAS

Durante el tiempo que estén vigentes, las contraseñas se almacenan de forma ininteligible mediante el propio sistema de encriptación que utiliza el Sistema Operativo.

IDENTIFICADORES Y CONTRASEÑAS SON PERSONALES E INTRANSFERIBLES

Los identificadores y contraseñas de acceso asignadas a cada usuario de la red corporativa de la Diputación, son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que se deriven del mal uso, divulgación o pérdida de los mismos.

PERIODICIDAD DE LAS CONTRASEÑAS

Las contraseñas de los usuarios autorizados se modifican con una periodicidad anual. Cada usuario será requerido por el Responsable de Seguridad la primera quincena hábil del año natural para que modifique las contraseñas. Durante el tiempo que estén vigentes, las contraseñas se almacenarán de forma ininteligible.

2.1.4. Control de acceso a las aplicaciones

Una vez dentro de la red el usuario podrá acceder o no a recursos, como las aplicaciones que tratan información de carácter personal, dependiendo de las autorizaciones particulares de cada usuario y de los grupos a los que pertenece.

Además del control a través de privilegios de acceso a los recursos de la red, existen ciertas aplicaciones que tienen su propio sistema de autenticación por contraseña, o que se encuentran en un servidor cuyo sistema operativo también proporciona un sistema de autenticación particular.

El sistema de control de acceso a las aplicaciones empleado en cada caso particular, se especifica en el **Anexo 2:** *"Relación de usuarios con acceso autorizado"*.

2.1.5. Control de acceso y confidencialidad de la información

Toda la información albergada en el sistema informático de la Diputación, de forma estática o en forma de mensajes de correo electrónico, es propiedad de la Entidad y tiene el carácter de confidencial. Por ello, todo el personal con acceso a datos de carácter personal firma el "Compromiso de Confidencialidad", según **Anexo 5.**

Sólo el Responsable del fichero podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por la dirección de la entidad.

2.1.6. Gestión de Soportes

Únicamente el Responsable de Seguridad podrá autorizar la salida de soportes informáticos que contengan datos personales, fuera de los locales en los que esté ubicado el fichero.

Los soportes informáticos, que contengan datos de carácter personal, permitirán identificar el tipo de información que contienen, ser inventariados y almacenarse en armarios protegidos con cerraduras con llave y con acceso regulado por el Responsable de Seguridad. El inventario de estos soportes se adjunta en **Anexo 4.**

Cuando un soporte que ha albergado datos de carácter personal vaya a ser reutilizado o desechado, se borra toda la información mediante su formateo o cualquier otro sistema que no permita su aprovechamiento. En el caso de que queden dudas sobre la información que pueda subsistir tras el proceso de borrado, se procederá a la inutilización física o a la destrucción del soporte.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

2.1.7. Origen de los Datos

Los datos con carácter personal provienen de: **Terceros y Personal de la institución**, que facilitan sus datos para la gestión de:

Los servicios ofrecidos por la entidad.

El pago de sus servicios.

La contratación, nómina y sus derivados.

Para garantizar la seguridad de estas fuentes y cumplir con los requisitos legales exigidos, los cuales salvaguardan los derechos de intimidad de los afectados, se establecen **cláusulas que recaban el consentimiento del afectado**, para todos los terceros y personal de la entidad.

Dentro de estas cláusulas, se contempla el informar a todos los afectados del tratamiento automatizado de sus datos, de los derechos que pueden ejercer por ser cedentes de datos, así como el nombre y dirección del Responsable del Fichero donde pueden ejercitar dichos derechos.

Así, la cláusula que se adjunta en los contratos/presupuestos de la entidad, establece:

PROTECCIÓN DE DATOS

El/Los firmantes queda/n informado/s de que los datos personales que se solicitan son necesarios para su formalización y gestión, y se incorporarán al correspondiente fichero de la DIPUTACIÓN para uso interno, y para la oferta, realización de operaciones y contratación de los servicios de la empresa, para lo cual da/n su autorización. El responsable de dicho fichero es la DIPUTACIÓN, cuyo domicilio figura en el presente documento, pudiendo el/los firmantes ejercitar los derechos de acceso, rectificación y cancelación de los datos obrantes en dicho fichero, en los términos establecidos en la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa complementaria. El/Los firmante/s presta/n por tanto su conformidad a la ***recogida*** *de datos, así como a la cesión, para las indicadas finalidades, que pueda ser realizada entre la Entidad y otras sociedades relacionadas con la contratación de los servicios de la empresa objeto de los servicios prestados por los mismos o auxiliares de éstos en los términos previstos en la indicada Ley.*

En cuanto a la cláusula que informa a los trabajadores de la entidad del tratamiento de sus datos y adjunta en todos los contratos de personal, es:

"De acuerdo con lo establecido en la Ley Orgánica 15/1999, el Trabajador, queda informado de la incorporación de sus datos a los ficheros existentes en la institución. Asimismo, queda informado del tratamiento a que van a ser sometidos todos sus datos a los que la Institución tenga acceso como consecuencia de la relación laboral, para las finalidades de gestión de nóminas y gestión de personal, así como cualquier otra gestión que genere dicha relación laboral. El Trabajador tiene derecho a oponerse al tratamiento de cualquiera de sus datos que no sean imprescindibles para la gestión de nóminas y gestión de personal y a su utilización para cualquier finalidad distinta del mantenimiento de la misma.

El Trabajador queda, igualmente informado sobre la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos en la legislación vigente. El responsable del fichero es: DIPUTACIÓN con domicilio en C/ Progreso 32 de Ourense, donde el afecto también se podrá dirigir por escrito en el caso de que lo encontrara necesario.

El Trabajador presta por tanto su conformidad a la recogida de datos, así como a la cesión para las indicadas finalidades que pueda ser realizada entre la Entidad y otras sociedades relacionadas con la gestión del personal de la institución (tales como entidades financieras, mutuas o entidades de seguro, ...) objeto de la relación laboral o auxiliares de éstas en los términos previstos en la indicada Ley."

2.1.8. Comunicación de Datos

La comunicación de datos debe estar autorizada, por lo que siempre que se comuniquen datos de carácter personal, se comprueba que se dirijan al propio afectado, o a entidades previamente autorizadas por el Responsable de Seguridad a través de su firma.

Identifica mediante una leyenda, el carácter de los datos.

Especifica claramente el destinatario autorizado para recibir y acceder a los datos.

Todo ello se consigue mediante la siguiente Leyenda, adjunta a todo soporte que de salida a datos de carácter personal de los ficheros de la Entidad

AVISO SOBRE CONFIDENCIALIDAD: ESTE DOCUMENTO O SOPORTE SE DIRIGE EXCLUSIVAMENTE A SU DESTINATARIO POR PODER CONTENER INFORMACIÓN CONFIDENCIAL O CUYA DIVULGACIÓN DEBE ESTAR AUTORIZADA EN VIRTUD DE LA LEGISLACIÓN VIGENTE. SE INFORMA A QUIEN LO RECIBIERA SIN SER EL DESTINATARIO O PERSONA AUTORIZADA POR ÉSTE, QUE LA INFORMACIÓN CONTENIDA EN EL MISMO ES RESERVADA Y SU UTILIZACIÓN O DIVULGACIÓN CON CUALQUIER FIN ESTÁ PROHIBIDA. SI HA RECIBIDO ESTE DOCUMENTO POR ERROR, LE ROGAMOS QUE NOS LO COMUNIQUE POR TELÉFONO Y PROCEDA A SU DESTRUCCIÓN.

En el caso en el que se contraten servicios externos que impliquen el acceso o utilización temporal de cualquier fichero de datos personales que se encuentren bajo la responsabilidad de la Diputación se procede según lo estipulado en IS-01-01 "Régimen de Contratación de Servicios Externos".

2.2. Funciones y Obligaciones del Personal

Normativa interna sobre la utilización de los equipos y servicios informáticos

La Diputación, con el fin de conseguir un eficaz cumplimiento de las funciones y obligaciones del personal mencionadas en el presente documento y relacionadas con la normativa vigente en materia de tratamiento de datos automatizados y seguridad de los sistemas informáticos, ha establecido un conjunto de normas internas que contemplan los deberes de los trabajadores en la utilización de los equipos y servicios informáticos de la institución. Dicho conjunto de normas se encuentra recogido en un documento de normas internas que es de obligado conocimiento y aceptación por parte de los trabajadores que tienen acceso a los

equipos y servicios informáticos. A continuación se mencionan, de forma resumida, las principales normas recogidas en dicho documento. Para más detalle, se adjunta una copia del documento de normas internas.

2.2.1. Obligaciones de todo el personal de la Diputación

Nombres de Identificación y Claves de Acceso

1. Queda prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso debe ponerlo en conocimiento del Responsable de Seguridad, con el fin de que le asigne una nueva clave. Ante una baja o ausencia temporal del usuario, el Responsable del Departamento puede solicitar al Responsable de Seguridad la creación de nuevos identificadores y claves de acceso a la persona por él designada.

2. El usuario está obligado a utilizar la red corporativa de la Diputación y sus datos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la entidad o de terceros, o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.

3. Todo usuario que realice una copia a disquete de cualquier información susceptible de contener datos de carácter personal debe solicitar la autorización o poner en conocimiento del Responsable de Seguridad, si así está contemplado en su trabajo diario, que se ha realizado tal copia, los datos que contiene y la finalidad de la misma.

4. Están **expresamente prohibidas** las siguientes actividades:

- Compartir o facilitar los identificadores de usuario y las claves de acceso facilitados por la Diputación con otra persona física o jurídica, incluido el personal de la propia entidad. En caso de incumplimiento de esta prohibición, el usuario es el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada el identificador del usuario.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la Diputación.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la Entidad o de terceros. (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal).
- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la entidad, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario.

- ntentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. (Esta actividad puede constituir un delito de interceptación de las telecomunicaciones, previsto en el artículo 197 del Código Penal).
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la Diputación o de terceros.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros. El usuario tiene la obligación de utilizar los programas anti-virus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la Diputación, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- Borrar cualquiera de los programas instalados legalmente.
- Utilizar los recursos telemáticos de la Entidad, incluida la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.
- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la entidad, en la red corporativa de la entidad.

Confidencialidad de la Información

1. Queda prohibido enviar información confidencial de la Diputación al exterior, mediante soportes materiales, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso.

2. Ningún colaborador debe poseer, para usos no propios de su responsabilidad, ningún material o información propiedad de la Entidad tanto ahora como en el futuro.

3. Los usuarios de los sistemas de información corporativos deben guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o entidades, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral con la Diputación y entidades relacionadas, tanto en soporte material como electrónico. Esta obligación continuará vigente tras la extinción del contrato laboral.

4. En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado entre en posesión de información confidencial bajo cualquier tipo de soporte, debe entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le irrogue derecho alguno de posesión, titularidad, copia o cobro de la referida información. Asimismo, el trabajador debe devolver dichos materiales a la enti-

dad, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación laboral. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de la entidad, no supone, en ningún caso, una modificación de este epígrafe.

5. El incumplimiento de esta obligación puede constituir un delito de revelación de secretos, previsto en el artículo 197 y siguientes del Código Penal y da derecho a la Diputación a exigir al usuario una indemnización económica.

Uso de Correo Electrónico

1. El sistema informático, la red corporativa y los terminales utilizados por cada usuario son propiedad de la Diputación.
2. Ningún mensaje de correo electrónico es considerado como privado. Se considera correo electrónico el dirigido o proveniente de otras redes públicas o privadas, y, especialmente, Internet. Todos estos mensajes van abiertos.
3. La Entidad se reserva el derecho de revisar, sin previo aviso, los mensajes de correo electrónico de los usuarios de la red corporativa, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la Entidad como responsable civil subsidiario.
4. Cualquier fichero introducido en la red corporativa o en el terminal del usuario a través de mensajes de correo electrónico que provenga de redes externas debe cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

Acceso a Internet

1. El uso del sistema informático de la Diputación para acceder a redes públicas como Internet, se limita a los temas directamente relacionados con la actividad de la Entidad y los cometidos del puesto de trabajo del usuario.
2. El acceso a debates en tiempo real (Chat / IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido.
3. El acceso a páginas web (WWW), grupos de noticias (Newsgroups) y otras fuentes de información como FTP, etc. se limita a aquéllos que contengan información relacionada con la actividad de la entidad o con los cometidos del puesto de trabajo del usuario.
4. La Diputación se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa.
5. Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet, debe cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

INCIDENCIAS

1. Es obligación de todo el personal de la Diputación comunicar al Responsable de Seguridad cualquier incidencia que se produzca en los sistemas de información a que tengan acceso.
2. Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.
3. Dicha comunicación debe realizarse inmediatamente, y, en cualquier caso, en un plazo de tiempo no superior a una hora desde el momento en que se conozca dicha incidencia.

PROTECCIÓN DE DATOS

Actos prohibidos:

1. Crear ficheros de datos personales sin la autorización del Responsable de Seguridad.
2. Cruzar información relativa a datos de diferentes ficheros o servicios con el fin de establecer perfiles de personalidad, hábitos de consumo o cualquier otro tipo de preferencias, sin la autorización expresa del Responsable de Seguridad.
3. Cualquier otra actividad expresamente prohibida en este documento o en las normas sobre protección de datos e Instrucciones de la Agencia de protección de Datos.

2.2.2. Funciones del Responsable del Fichero

Nombre del responsable del fichero: DIPUTACIÓN.

Funciones:

1. Notificar a la Agencia de Protección de Datos los ficheros de datos personales de la entidad.
2. Velar por el cumplimiento de todos los requisitos establecidos en la LOPD y en Reglamento de Seguridad.
3. Redactar, establecer y comprobar la aplicación y el cumplimiento del documento de seguridad.
4. Describir los sistemas de información que realizan el tratamiento de los datos personales de la entidad.
5. Describir la estructura de los ficheros de la entidad.
6. Establecer los criterios que el Responsable de Seguridad debe seguir al realizar la función de conceder, alterar o anular el acceso autorizado a los datos y recursos.
7. Establecer los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
8. Nombrar uno o varios Responsables de Seguridad, encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso, esta designación supone una delegación de la responsabilidad que corresponde al Responsable del Fichero.
9. Adoptar las medidas correctoras adecuadas, en función del análisis de los Informes de Incidencias realizados por el Responsable de Seguridad.
10. Establecer un mecanismo que permita la identificación inequívoca y personalizada de todo aquél usuario que intente acceder al sistema y la verificación de que está autorizado.
11. Establecer y comprobar la aplicación de una medida que impida el intento reiterado de acceder de forma no autorizada al sistema de información.

2.2.3. Funciones del Responsable de Seguridad

Nombre del responsable de seguridad: El Jefe del servicio de Informática y Nuevas Tecnologías o, en su ausencia, el Técnico en redes y seguridad.

Funciones:

1. Velar por el cumplimiento de las normas de seguridad contenidas en el Documento de Seguridad.

2. Recopilar y describir las medidas, normas, procedimientos, reglas y estándares de seguridad adoptados por la entidad.

3. Determinar el ámbito del documento de seguridad

4. Determinar y describir los recursos informáticos a los que se aplica el documento de seguridad.

5. Establecer y comprobar la aplicación del procedimiento de notificación, tratamiento y registro de incidencias.

6. Establecer y comprobar la aplicación del procedimiento de realización de copias de respaldo y recuperación de datos.

7. Comprobar el cumplimiento de la periodicidad establecida para la realización de copias de respaldo.

8. Elaborar y mantener actualizada la lista de usuarios que tengan acceso autorizado al sistema informático de la entidad, con especificación del nivel de acceso que tiene cada usuario.

9. Establecer y comprobar la aplicación del procedimiento de identificación y autenticación de usuarios.

10. Establecer y comprobar la aplicación del procedimiento de asignación, distribución y almacenamiento de contraseñas.

11. Comprobar el mantenimiento de la confidencialidad de las contraseñas de los usuarios.

12. Establecer y comprobar la aplicación del procedimiento de cambio periódico de las contraseñas de los usuarios.

13. Establecer y comprobar la aplicación de un procedimiento que garantice el almacenamiento de las contraseñas vigentes de forma ininteligible.

14. Establecer y comprobar la aplicación de un sistema que limite el acceso de los usuarios únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

15. Establecer y comprobar la aplicación de los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.

16. Conceder, alterar o anular el acceso autorizados a los datos y recursos, de acuerdo con los criterios establecidos por el responsable del fichero.

17. Establecer y comprobar la aplicación de un sistema que permita identificar, inventariar y almacenar en lugar seguro los soportes informáticos que contienen datos de carácter personal.

18. Autorizar la salida de soportes informáticos que contengan datos de carácter personal.

19. Velar por el cumplimiento de las normas de seguridad, comunicando al Responsable del Fichero las infracciones cometidas, para el establecimiento de las correspondientes sanciones.

20. Establecer y comprobar la aplicación de controles periódicos para verificar el cumplimiento de lo dispuesto en el documento de seguridad.

21. Coordinar y controlar las medidas definidas en el documento de seguridad.

22. Establecer y comprobar la aplicación de las medidas necesarias para impedir la recuperación posterior de la información almacenada en los soportes informáticos que van a ser desechados o reutilizados, o que vayan a salir fuera de los locales en que se encuentran ubicados los ficheros.

23. Hacer el seguimiento del registro de incidencias y ampliar los campos del mismo para dejar constancia de los procedimientos realizados para la recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos han sido necesarios grabar manualmente en el proceso de recuperación.

24. Autorizar por escrito la ejecución de los procedimientos de recuperación de datos.

25. Comprobar que en la fase de pruebas de los sistemas de información, éstas no se efectúen con datos personales reales.

2.3. Estructura de los Ficheros con Datos de Carácter Personal y descripción de los Sistemas de Información que los tratan

En el **Anexo 7** se describe la estructura de los ficheros automatizados con datos de carácter personal de la DIPUTACIÓN.

Notas aclarativas sobre la interpretación de las fichas que describen los ficheros:

- En el campo ***Ubicación del Fichero*** se especifica la localización física del fichero dentro de la red corporativa de la institución según el siguiente formato:

  Nombre de red del equipo \ directorio \ subdirectorio

- En el campo ***Departamentos que tienen acceso a las aplicaciones***, se especifican los departamentos que tienen acceso habitual a las aplicaciones que trabajan con ficheros de datos de carácter personal. No obstante, también se puede producir la necesidad de un acceso esporádico por parte del departamento de Informática y Nuevas Tecnologías por razones de mantenimiento de las aplicaciones.

2.4. Procedimiento de notificación, gestión y respuesta ante las incidencias

La DIPUTACIÓN dispone de un procedimiento de notificación, gestión y respuesta de las incidencias, entendiendo por "incidencia" cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, tales como pérdida o deterioro de datos en cualquier transmisión, caída de los Sistemas informáticos, pérdida de cualquier soporte físico o automatizado que pudiera contener datos de carácter personal,…

2.4.1. Notificación

Cualquier persona que forme parte de la plantilla de la entidad o se halle prestando sus servicios temporalmente en la misma notifica inmediatamente al Responsable de Seguridad cualquier anomalía que detecte y que afecte o pueda afectar a la seguridad de los datos, con la máxima celeridad y en un plazo siempre inferior a una hora desde su detección.

2.4.2. Gestión

El Responsable de Seguridad recibe las notificaciones de incidencias, se las comunica al Responsable del Fichero, así como a los técnicos internos o externos encargados de la Seguridad del Sistema, para que conozcan el alcance de las mismas, y procede a su registro.

2.4.3. Respuesta

El Responsable de Seguridad se asegura de que los técnicos dan respuesta inmediata a la incidencia detectada y supervisa el trabajo de subsanación de la anomalía detectada.

2.4.4. Registro

El Responsable del Fichero, de conformidad con el artículo 10 del Real Decreto 994/1999, ha creado un registro "Informe de Incidencias" (**Anexo 6**) en soporte papel en el cual se hace constar la siguiente información relativa a las incidencias:

- Nombre, Nivel y Responsable del Fichero en el que se produce la Incidencia.
- Documento de Seguridad referido por el Fichero.
- Persona que detecta la Incidencia.
- Descripción de Incidencia.
- Acciones a Emprender (Preventivas o Correctoras), Persona responsable de la acción.

El Responsable de Seguridad realiza un seguimiento de las acciones correctoras y/o preventivas establecidas, y se asegura de que éstas se apliquen lo más rápidamente posible hasta que se resuelva la incidencia detectada.

Es obligación del Responsable de Seguridad mantener actualizado el registro de incidencias.

En el Informe de Incidencias se consignan, 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.

Para la ejecución de los procedimientos de recuperación se precisa la autorización por escrito del Responsable del Fichero.

2.5. Procedimiento de realización de Copias de Respaldo y Recuperación de Datos

Sólo se realizan el número mínimo de copias de seguridad que son necesarias.

Cuando existen varias copias de un mismo fichero, archivo, grupo de registros, datos, grupo de datos de carácter personal sometidos a control, independientemente del soporte en el que estén, se tratan con el mismo rigor que si fueran copias de seguridad.

En el **Anexo 8** se presenta la relación de sistemas y fuentes de datos que son objeto de las operaciones de copia de seguridad realizadas en la institución. Así mismo, también se especifica en dicho anexo el procedimiento a seguir para configurar las operaciones de copia de seguridad y los correspondientes procedimientos de restauración de los datos.

El Responsable de Ficheros designa al "Encargado de copias" como personal autorizado para la realización de las copias de seguridad.

Todos los soportes derivados de estas copias de seguridad están incluidos en el "Inventario de Soportes", conforme al **Anexo 4** anteriormente mencionado, estableciéndose su ubicación y la persona encargada de su custodia a efectos de su control.

Otros Sistemas de Tratamiento de Información

La información de carácter personal de **Fichas de Clientes, Contratos, Nóminas** y otros documentos similares en soporte papel, relacionados con los clientes y personal de DIPUTACIÓN se encuentran en los departamentos específicos que requieran tal información.

ANEXOS

ANEXO I

RELACIÓN DE PUESTOS DE TRABAJO QUE REALIZAN FUNCIONES SOBRE MEDIDAS DE SEGURIDAD

PUESTO DE TRABAJO	FUNCIONES
Jefe de Informática y Nuevas Tecnologías	Elaborar y coordinar las medias de seguridad descritas en el Documento de Seguridad
Técnico en Redes y Seguridad	Velar por el cumplimiento de las normas de seguridad contenidas en el Documento de Seguridad
Jefes de Departamento	Autorizar las operaciones necesarias para el tratamiento de los datos de carácter personal así como la salida de cualquier tipo de soporte que contenga dichos datos
Usuarios de Departamento	Realizar las operaciones necesarias para el tratamiento de datos de carácter personal autorizadas por el correspondiente Jefe de negociado
CONCLUSIONES: En ausencia del Jefe de Informática y Nuevas Tecnologías, sus funciones son asumidas por el Técnico de redes y seguridad	**Fecha : 20/05/2006**

ANEXO II

RELACIÓN DE USUARIOS CON ACCESO AUTORIZADO

ÍNDICE

NOMBRE DEL FICHERO: *nombre_fichero*			**RESPONSABLE DEL FICHERO:** *nombre_institución*	
DOCUMENTO DE SEGURIDAD: DS_DPO				
A continuación se relacionan los usuarios autorizados para acceder al sistema de información de la institución. Esta relación se actualizará cada vez que se produzca un cambio.				
DEPARTAMENTO / USUARIO AUTORIZADO	**VÍA DE ACCESO**	**CONTROL DE ACCESO**	**PERMISOS**	**PRIVILEGIOS ESPECIALES**
DEPARTAMENTO (Nombre del departamento que trabaja con el fichero)				
Especificar los usuarios que tienen acceso al fichero.	Especificar el nombre de la aplicación con la que se trabaja sobre el fichero.	Especificar cómo se lleva a cabo el control de acceso al fichero y los privilegios del mismo.	Tipo de permiso: lectura, escritura, ejecución, etc.	Indicar se existen privilegios específicos para el fichero.
DEPARTAMENTO (Nombre del departamento que elabora y gestiona el fichero)				
Especificar los usuarios que elaboran y gestionan el fichero.	Especificar el nombre de la herramienta que ha sido utilizada por el desarrollador.	Especificar cómo se lleva a cabo el control de acceso al fichero y los privilegios del mismo.	Tipo de permiso: lectura, escritura, ejecución, etc.	Indicar se existen privilegios específicos para el fichero.
	Especificar el lenguaje, herramienta y tipo de sistema utilizado por el desarrollador.		Tipo de permiso: lectura, escritura, ejecución, etc.	
CONCLUSIÓN DEL RESPONSABLE DEL FICHERO:			**Fecha : 20/05/2006**	

Nota:

Hay que cumplimentar una ficha como ésta por cada fichero que se haya registrado en la Agencia de Protección de Datos. A continuación, se presenta una relación de los ficheros que la Excma. Diputación Provincial de Ourense tiene dados de alta, de los que haremos una ficha como la que se acaba de presentar.

A modo de ejemplo, se indican alguno de los ficheros que la Excma. Diputación Provincial de Ourense, tiene dados de alta en la Agencia de Protección de Datos. Esta información es de carácter público, y puede ser consultada en la página de la Agencia.

1. Recursos Humanos
2. Contabilidad
3. Riesgos Laborales
4. Asistencia Social
5. Formadores

Anexo III

Estructura general del Sistema Informático

EQUIPO: *nombre_servidor (nombre_sistema)* (Especificar el nombre del sistema informático concreto)

Descripción

Breve resumen en el que se especifica el tipo de Sistema Informático que se encuentra instalado en la Institución. Es necesario indicar el tipo de máquina, funcionalidad, actividad para la que se destina, el sistema de red al que pertenece, etc.

Sistema Operativo

Indicar el tipo de Sistema Operativo que se encuentra instalado en cada equipo informático que configura la red.

Nombre de red

Nombre con el que se designa la red a la que pertenece cada equipo informático concreto.

Tipo de acceso desde los equipos de la Red

Especificar cómo se sostiene la accesibilidad por parte de los equipos a la Red que constituye el Sistema Informático de la Institución.

Situación física

Breve descripción ámbito físico en el que se encuentra cada equipo informático concreto.

Nota:

Es necesario cumplimentar los apartados anteriores por cada dispositivo que constituya el Sistema Informático de la institución.

ANEXO IV

INVENTARIO DE SOPORTES

TIPO SOPORTE	IDENTIFICACIÓN	EQUIPO	UBICACIÓN	FICHEROS	RESPONSABLE
Nombre del Soporte	Número del Dispositivo y Nombre Etiqueta	Nombre del Sistema	Nombre Localización	Lista de ficheros que guarda el dispositivo	Responsable de Seguridad

Nota:

Es necesario cumplimentar los datos de la tabla para cada uno de los soportes informáticos que existan en cada institución en concreto. Lo que se pretende es elaborar una relación de todos los dispositivos que constituyen el Sistema Informático de la misma.

ANEXO V.

COMPROMISO DE CONFIDENCIALIDAD

Don/Doña:

Se compromete, durante su relación laboral con la DIPUTACIÓN a:

- Conocer y cumplir lo establecido en el Documento de Seguridad de Datos Personales así como en otros documentos de régimen interior en la medida que le sean aplicables, por la naturaleza de las actividades, funciones y responsabilidades que se le encomienden.
- No realizar ninguna actividad que sea incompatible con su independencia de juicio e integridad profesional en relación con las actividades de la DIPUTACIÓN.
- Mantener absoluta confidencialidad y discreción sobre la información obtenida en el ejercicio de su trabajo acerca de las actividades de la institución, de sus clientes, personal y organismos relacionados. Especialmente en lo que se refiere a Datos de Carácter Personal, incluso tras la extinción de su relación laboral con la Entidad.
- Observar y cumplir los criterios establecidos en el Documento de Seguridad, en lo que se refiere a "Funciones y Obligaciones del Personal".

En Ourense, a de de

Firmado:

ANEXO VI

INFORME DE INCIDENCIAS

NOMBRE DEL FICHERO:	NIVEL DELFICHERO:	☐ Básico ☐ Medio ☐ Alto
DOCUMENTO DE SEGURIDAD: DS_DPO		
DETECTADA POR:	RESPONSABLE DEL FICHERO:	
DESCRIPCIÓN:		
ACCIONES A EMPRENDER	CIERRE DE LAS ACCIONES	
ACCIÓN ☐ Preventiva ☐ Correctora Descripción: Responsable de la acción:	Fecha Cierre: / / Firma del responsable:	
ACCIÓN ☐ Preventiva ☐ Correctora Descripción: Responsable de la acción:	Fecha Cierre: / / Firma del responsable:	
ACCIÓN ☐ Preventiva ☐ Correctora Descripción: Responsable de la acción:	Fecha Cierre: / / Firma del responsable:	
Si la acción a tomar implicase la recuperación de datos, ésta se realiza conforme al Procedimiento de Realización de Copias de Respaldo y Recuperación de Datos, describiendo la persona que realiza el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.		
CONCLUSIÓN DEL RESPONSABLE DEL FICHERO:	Firma del Responsable del Fichero: Fecha : / /	

ANEXO VII

ESTRUCTURA DE LOS FICHEROS CON DATOS DE CARÁCTER PERSONAL

NOMBRE DEL FICHERO: *nombre_fichero* (Especificar el nombre del fichero concreto)

Nivel de Seguridad

Tipo de seguridad que se aplica al fichero. Existen tres niveles:

- **Bajo:** Ficheros sin datos de carácter personal.
- **Medio:** Ficheros con datos personales, pero que no presentan un nivel de máxima seguridad.
- **Alto:** Ficheros con datos de carácter personal a los que se les aplica máxima seguridad, por disponer de datos relacionados con salud, religión, sexo, etc.

Código de inscripción en la Agencia de Protección de Datos

Indicar el código de inscripción que le ha sido asignado por la Agencia de Protección de Datos.

Fecha de publicación en el B.O.P.

Especificar la fecha de publicación del B.O.P, en el que se manifiestan los ficheros que se van a dar de alta en la Agencia de Protección de Datos.

Finalidad y usos previstos

Breve resumen en el que se especifica el objetivo para el que se crea cada fichero, así como la utilidad para la cual ha sido destinado.

Personas o colectivos sobre los que se obtendrán datos

Enumeración de las personas o grupos de los que se van a tratar datos de carácter personal.

Procedimiento de recogida de datos

Indicar el proceso que se sigue para obtener los datos de carácter personal que se van a tratar en cada fichero.

Estructura básica del fichero

Breve resumen que describe cómo es la estructura de los ficheros que contienen datos de carácter personal, que han sido dados de alta en la Agencia de Protección de Datos.

Ubicación del fichero

Especificar la ruta en la que se encuentra localizado el fichero.

Aplicaciones utilizadas en el tratamiento del fichero

Indicar las aplicaciones que se utilizan para tratar los ficheros.

Departamentos que tienen acceso a las aplicaciones

Enumerar los departamentos de la entidad a los que se le concede el acceso a las aplicaciones que tratan con los ficheros registrados en la Agencia de Protección de Datos.

Cesiones de datos previstas a terceros

Indicar si se produce la cesión de datos de los ficheros a terceros.

Nota:

Es necesario cumplimentar los apartados anteriores por cada fichero que haya sido dado de alta en la Agencia de Protección de Datos.

ANEXO VIII

COPIAS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Configuración de los procesos automáticos de copia en el sistema *nombre_sistema*

En este apartado hay que describir la planificación que se establece para realizar copias de seguridad de forma automática. Además hay que indicar la frecuencia con la que se lleva a cabo este proceso (diaria, mensual, anual, etc.)

2. Procedimiento manual de copia de seguridad en el sistema *nombre_sistema*

Realizar un breve resumen de los pasos que hay que seguir para llevar a cabo una copia de seguridad de forma manual.

3. Procedimiento de restauración de los datos en el sistema *nombre_sistema*

En esta sección hay que redactar minuciosamente cómo se lleva a cabo el proceso de restauración que hay que seguir, en el caso de que se produzca la pérdida o corrupción de información que se almacena en los sistemas informáticos de la entidad.

Nota:

En la sección de *Copias de Respaldo y Recuperación de Datos*, hay que describir cómo son el proceso automático y manual de copias, así como el procedimiento que hay que seguir para la restauración de los datos en caso de pérdida o corrupción de la información. Para presentarlo de forma más clara y precisa, se han elaborado tres apartados en los que cada institución debe especificar cómo lleva a cabo cada uno de los procedimientos citados.

Notas Sobre el Documento

El presente documento es un ejemplo del ***Documento de Seguridad de la Excma. Diputación Provincial de Ourense***. Se ha diseñado con la finalidad de desarrollar un modelo que pueda ser utilizado por otras instituciones, en las que se maneje información del mismo tipo y que dispongan de un sistema informático similar.

En todas las fichas y puntos que se presentan, se han utilizado nombres genéricos resaltados en cursiva (que habría que cambiar por los datos pertinentes, para cada institución que utilice dicho modelo). Además, en cada apartado se ha explicado de la forma breve, clara y concisa, qué datos deben ser suministrados en cada caso.

Edita

Formación Continua
DEPUTACIÓN OURENSE

Presidente
José Luis Baltar Pumar

Jefe de Negociado de Formación
y Coordinador de la Publicación
Carlos Castiñeiras Rois

Autor de la Publicación
©Álvaro Gómez Vieites

Textos Anexos
©Servicio de Informática
y Nuevas Tecnolgías de la
Deputación de Ourense

Supervisión Técnica
José Antonio González Cid

Supervisión Lingüística
Ana Vázquez Pereira

Diseño
Nácher Publicidad

Imprime
C/A GRÁFICA

I.S.B.N.
84-96503-35-6

Dep. legal

DEPUTACIÓN PROVINCIAL
DE OURENSE

Formación Continua
DEPUTACIÓN OURENSE

Ministerio de Administraciones Públicas
Instituto Nacional de Administración Pública

FUNDACION CAIXAGALICIA

Acuerdo de Formación Continua en las Administraciones Públicas

Negociado de Formación da Deputación de Ourense • Rúa Progreso, Nº 30, 2º - 32003 OURENSE
Teléfono: 988 385 142 - Fax: 988 385 215 - e-mail: formacion@depourense.es - web: www.depourense.es