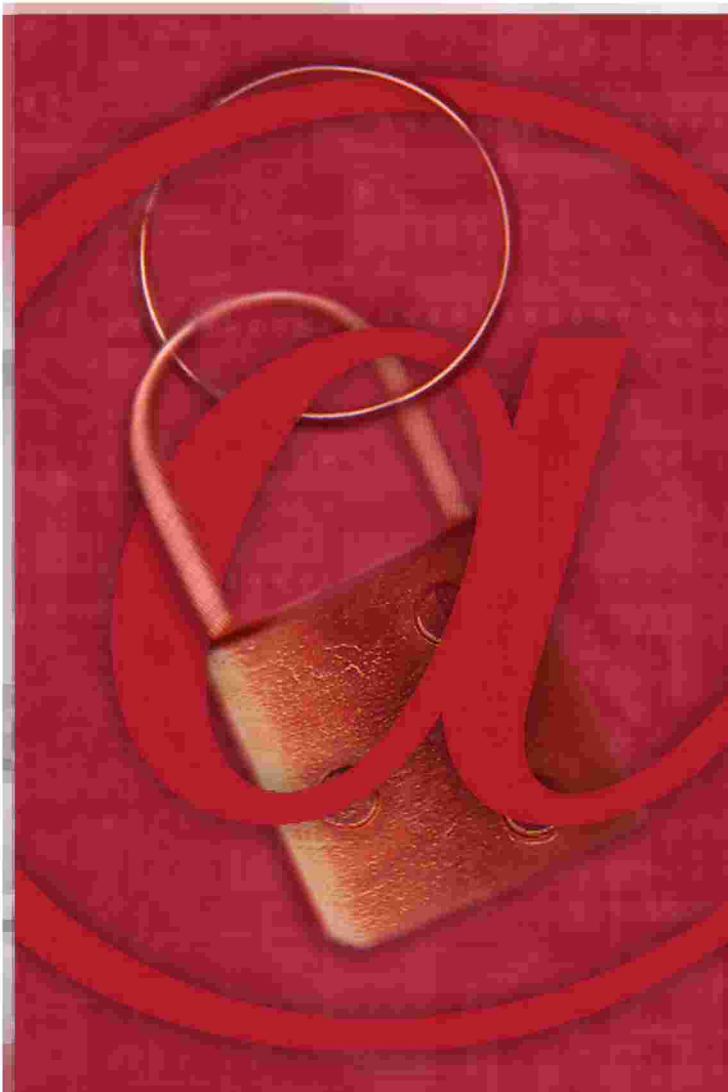
Protección de datos y PYMES



anetcom

Protección de datos y PYMES

anetcom

Edita:
Anetcom

Creación de contenidos:
Rafael Alonso. Socio Director "SSI Sistemas"

Coordinación:
José Luis Colvée

Revisión:
Inmaculada Elum
Juan Antonio Pardo

Diseño, Composición e impresión:
Filmac Centre, S.L.

Depósito legal:
V-2708-2004

Índice

Prólogo

Desde la Conselleria de Empresa, Universidad y Ciencia entendemos que es necesario motivar al empresariado sobre el cumplimiento de las normativas que afectan a su negocio y cuyo incumplimiento puede generar grandes inconvenientes en el desarrollo del mismo. Por otra parte, las exigencias de la Sociedad de la Información en la que estamos inmersos aumenta la preocupación por la protección del derecho a la intimidad de las personas.

Bajo este doble prisma de conciencia social y responsabilidad empresarial, ANETCOM, Asociación que tengo el honor de presidir, publica el tercero de los ejemplares de su Línea Editorial: "Protección de datos y PYMES".

Esta publicación presenta una guía práctica para que el empresario pueda conocer cómo adaptarse a la normativa de protección de datos y, de este modo, colaborar en la salvaguarda del derecho a la intimidad y paliar la utilización abusiva e indiscriminada de los datos personales con fines comerciales, en medios publicitarios o de comunicación.

La aparición de la Ley 15/1999, Ley Orgánica de Protección de los Datos de Carácter Personal, más conocida como LOPD, ha supuesto un hito importante por cuanto ha venido a fijar los límites en la obtención, utilización y difusión de los datos personales por las empresas y profesionales de nuestro país o que desarrollan su actividad en él, regulando el uso y la difusión de cualquier información que se refiera a las personas físicas. Asimismo, el Reglamento de Medidas de Seguridad de los datos automatizados de carácter personal, desarrollado por el Real Decreto 994/1999, ha establecido las medidas y controles de seguridad que deben establecerse en los sistemas que traten informáticamente datos personales. La obligación de adaptar dichos sistemas informáticos al Reglamento afecta por igual a profesionales y empresas, con independencia de su tamaño, del tipo de actividad o del sector en que la realicen.

Por todo ello la presente obra, basada en el principio de que los riesgos sobre los datos de carácter personal son mayores a causa de las personas que a causa de los sistemas de información, hace un significativo énfasis en la importancia de implicar a los usuarios en la seguridad y buen uso de la información de carácter personal.

Justo Nieto Nieto
Conseller de Empresa, Universidad y Ciencia
de la Comunidad Valenciana

Introducción

Con la promulgación el 14 de diciembre de 1999 de la Ley Orgánica 15/1999, de protección de Datos de Carácter Personal, se culmina el ciclo iniciado en 1992 con aparición la de la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de Datos de carácter personal, mas conocidad como LORTAD. Durante este periodo la preocupación del legislador ha sido poner límites a la utilización indiscriminada, abusiva y en ocasiones fraudulenta de los datos de los ciudadanos.

Ya en 1992, la promulgación de la LORTAD, puso de manifiesto dos hechos significativos: de una parte la importancia creciente de los sistemas de información en el tratamiento y almacenamiento de información relativa a las personas, y de otra parte la facilidad con que dicha información podía ser transferida entre los sistemas que la gestionaban, sin limitación geográfica ni temporal y con ello la necesidad de dotar a estos de un serie de controles que limitasen su utilización.

Si en un principio la preocupación del legislador parecía centrase en los sistemas de mayor riesgo, así se puede deducir de la publicación de la Instrucción 1/1995, de la Agencia de Protección de Datos, *relativa a prestación de servicios de información sobre solvencia patrimonial y crédito*, lo que apuntaba de forma clara a la información tratada por las entidades financieras; nada más lejos de la realidad.

La aparición en los siguientes años de la *Instrucción 1/1996, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios*, y de la *Instrucción 2/1996*, de la citada Agencia de Protección de Datos, *sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los Casinos y Salas de Bingo*, ponían claramente de manifiesto su preocupación por la protección de la intimidad

de los ciudadanos en su sentido más estricto, en la línea de lo establecido en la Carta Constitucional.

Así ha quedado ratificado por la Ley 15/1999, más conocida como LOPD, en cuyo artículo 1, al referirse al objeto de la misma dice: *"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."*

Por tanto, nos encontramos ante una norma superior de obligado cumplimiento para todo aquel que tenga acceso y capacidad para gestionar datos personales de terceros con cualquier finalidad que exceda del ámbito particular y doméstico.

Resulta frecuente escuchar en el ámbito empresarial comentarios tales como 'la adaptación a la LOPD es una cuestión de los informáticos' o bien 'nuestra empresa es muy pequeña y por nuestra actividad no tenemos datos personales'.

Ambas afirmaciones, así como tantas otras similares, son totalmente erróneas. Toda empresa, con independencia de su tamaño y actividad, gestiona datos de carácter personal. El que lo dude simplemente tiene que dar una mirada a las nóminas de sus empleados o a las fichas de sus proveedores y clientes.

En cuanto a la primera afirmación, también es errónea: Los riesgos de una utilización indebida de los datos personales dependen en mayor medida las personas que de los sistemas informáticos[1], basta recordar los expedientes abiertos por el Agencia de Protección de Datos a empresas que habían depositado en los contenedores de residuos listados de empleados, resultados de pruebas de evaluación de candidatos o incluso currículums con valoraciones 'poco elegantes' hechas por los entrevistadores.

Así pues, adaptarse a la Normativa de Protección de Datos, esto es, cumplir con la Ley 15/1999, la LOPD, y con el Reglamento de Medidas de

[1] Para más información se pueden consultar los informes que el CSI/FBI Computer crime & security survey viene elaborando a nivel mundial desde hace nueve años. (www.gocsi.com)

Seguridad que establece el Real Decreto 994/1999, es una obligación que afecta a todas las empresas y profesionales que realizan su actividad con carácter público.

Esta guía para Pymes pretende facilitar a los responsables de estas empresas dicha adaptación desde un enfoque práctico, de la forma más sencilla, más económica y en el menor plazo de tiempo. Lejos de profundizar en los aspectos jurídicos de ambas normas, sus capítulos intentan poner de manifiesto aquellos aspectos de seguridad y buenas prácticas que la empresa debe tener presentes en los procesos de obtención, gestión y almacenamiento de los datos personales, así como en su transmisión, cesión o tratamiento por terceros.

Para facilitar la utilización de la guía, cada capítulo hace referencia a una de las normas. Así, el capítulo primero se refiere a los requisitos necesarios para cumplir con la LOPD, el capítulo segundo hace referencia a las medidas de seguridad a implantar según el R.D. 994/1999. El capítulo tercero está dedicado a la Agencia de Protección de Datos y a sus diferentes competencias y actuaciones. En el capítulo cuarto se presentan de forma ordenada las acciones a realizar por la Pyme para adaptarse a ambas normas.

También se ha incluido en esta guía un pequeño glosario de términos que facilitan la comprensión de los diversos conceptos a que hacen referencia la citadas normas.

Confiamos que de su lectura surjan las mejores ideas para la aplicación práctica de los mecanismos de seguridad proporcionales y adecuados a la información personal gestionada por el lector.

1. Cumplimiento de la Ley Orgánica de Protección de Datos 15/1999

1.1 Objeto y ámbito de aplicación

El artículo 1 de la LOPD, al que ya nos hemos referido con anterioridad, establece que el objeto de la Ley 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.'* De ello hemos de deducir que quien vaya a gestionar datos de personas físicas deberá hacerlo de forma que su actuación no suponga riesgos para aquellas.

La Ley, en su artículo 2, establece que es 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.'*

Hemos de entender con ello que están amparados por la Ley los datos personales que cualquier empresa o profesional posee y gestiona como consecuencia de su actividad cotidiana, con independencia del soporte físico en que se encuentre dicha información, bien sea papel, microfilm, microfichas, discos de ordenador, cintas magnéticas, disquetes, CDs, DVDs, así como cintas de video, películas o fotografías.

En las empresas, además de la información de carácter personal relativa a los empleados, existen otros datos que también pueden ser considerados como datos de carácter personal en los términos de la Ley[2], así con independencia de que los clientes y/o proveedores de la empresa sean personas jurídicas, es habitual que en las fichas, registros, correspondencia y demás documentación estén identificadas personas físicas y los puestos que estas ocupan en las citadas empresas. Ello constituye un dato personal, toda vez que dichas personas físicas 'son identificables'.

[2] Ver definición de dato personal en el Glosario

En el ámbito laboral se tiende con frecuencia en las empresas se tiende a simplificar el alcance de la Ley exclusivamente a la información contenida en las nóminas y contratos de los empleados. Téngase en cuenta que cualquier documento relacionado con un empleado y sus familiares (sanciones, permisos, situaciones de baja, cambios de su estado civil, nuevos hijos, formación y calificaciones, etc.), son también datos de carácter personal; como también lo son su dirección de correo electrónico o su agenda de citas.

Los historiales, currículums, solicitudes de empleo, candidaturas, etc, son documentos que habitualmente contienen abundantes datos personales de quienes los remitieron, por ello deben ser considerados como información personal y gestionados adecuadamente, ya que de lo contrario pueden ocasionar desagradables consecuencias para la empresa.

◆ 1.2 Operaciones con los datos

Las operaciones que dentro de la gestión de la empresa Pyme se realizan en relación con los datos de carácter personal las podemos agrupar en cinco: obtención de los datos, tratamiento de los mismos, almacenamiento o archivo, comunicación a terceros y destrucción. Veamos qué requisitos impone la LOPD en cada una de dichas operaciones:

1.2.1. Obtención de los datos o adquisición

Entenderemos por tal el proceso por el cual la empresa alcanza la posesión de los datos personales de clientes, proveedores, empleados, etc., para su explotación posterior.

Las vías más habituales para obtener dichos datos suelen ser la relación personal, tarjetas de visita, fichas de visitantes a exposiciones, visitas de los comerciales de la empresa, compras de bases de datos, etc.

En relación con la obtención de los datos, el artículo 4 de la Ley establece: *'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'.*

Por tanto, la empresa deberá de cuidar que los datos recogidos sean los estrictamente necesarios para asegurar la correcta relación entre las partes, y la utilización de dichos datos sea la que corresponde a los fines para los que éstos fueron recogidos.

En relación con los datos personales obtenidos a través de la adquisición de bases de datos a empresas comercializadoras de éstas, la empresa compradora deberá de obtener del vendedor la garantía de que los datos contenidos en la base de datos han sido obtenidos por los medios y con las autorizaciones previstas por la LOPD. En caso de que el comprador no obtenga dicha garantía, preferiblemente por escrito, podría verse implicado en una infracción por uso inadecuado de datos personales.

Así mismo, el artículo 5 de la Ley establece que: *'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.'*

El cumplimiento de estas obligaciones no siempre resulta sencillo, dadas las dificultades técnicas que pueden presentarse. Veamos algunas de ellas:

Con los datos personales obtenidos como consecuencia de la relación personal en la que se produce la entrega de tarjetas de visita, si estos datos van a ser incorporados a un fichero o serán objeto de un tratamiento posterior, (por ejemplo su incorporación a una agenda o a un fichero informático de contactos) se deberá informar a la otra parte de que tal procedimiento se va a realizar. Además, resulta una buena práctica conservar las tarjetas de visita como elemento de prueba ante una posible necesidad de demostrar cómo se obtuvieron dichos datos.

Si los datos se han obtenido por medio de fichas de asistentes a las instalaciones de la empresa o a ferias y exposiciones en las que esta participa, es conveniente que en dichos formularios se incluya de forma clara la información sobre la finalidad y el tratamiento de que serán objeto los datos que se están recogiendo, así como también se deberán indicar los derechos que puede ejercitar esta persona en relación con lo datos que nos está facilitando.

En el caso de recogida telefónica de datos personales, en el que resulta difícil demostrar que la otra parte ha sido informada del tratamiento que se dará a sus datos y también de sus derechos sobre tales datos, puede ser una buena práctica la confirmación escrita de la conversación, vía correo electrónico, fax o carta, incluyendo tal información.

De forma similar deberíamos actuar con relación a los currículums recibidos por correo, fax o correo electrónico, indicando además cuál será el plazo durante el que conservaremos los datos en nuestros archivos y ofreciendo la posibilidad de destruirlos antes de ese plazo si el interesado nos lo indica así.

1.2.2. Tratamiento

Entendemos por tratamiento de los datos aquellas operaciones realizadas sobre éstos para su gestión. Tales operaciones incluyen la introducción en sistemas informáticos, la creación de carpetas o expedientes, así como su copia, transmisión a través de medios de comunicación, archivado y custodia.

El artículo 6 de la LOPD establece la necesidad de obtener el consentimiento inequívoco del afectado para el tratamiento de sus datos, salvo que la Ley imponga otra cosa.

En el mismo artículo se indica que: *'No será preciso el consentimiento… 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…'.*

Basándonos en ello podemos considerar que todos los datos de clientes, proveedores o empleados existentes en la Pyme tienen como finalidad el mantenimiento de relaciones de negocio, laborales o administrativas y, por ello, su tratamiento, dentro de este ámbito, no requiere de consentimiento de los afectados.

Sin embargo este criterio no sería aplicable en el caso utilización de los datos de un cliente para ofrecerle productos o servicios de otra empresa diferente a aquella con la que mantiene la relación comercial, aunque la segunda empresa forme parte del mismo grupo, pues en tal caso dichos datos están siendo tratados para una finalidad distinta de aquella para la que fueron obtenidos.

El afectado puede en todo momento revocar el consentimiento en uso de sus derechos. Dicha revocación debe ser atendida por la empresa y no tiene efectos retroactivos.

Así mismo el afectado puede oponerse al tratamiento de sus datos, siempre que existan motivos fundados y legítimos, aún cuando el tratamiento de dichos datos no hubiera requerido de su consentimiento previo.

La empresa deberá poner especial atención en el tratamiento de los datos especialmente protegidos, entendiéndose por tales los datos relacionados con la ideología, afiliación sindical, religión, creencias, origen racial o étnica, o vida sexual.

El artículo 7 de la Ley 15/1999 prohíbe el tratamiento de los datos relativos a la ideología, afiliación sindical, religión, creencias sin el consentimiento expreso del afectado.

También se establece en dicho artículo la prohibición de crear ficheros 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.

En cuanto a los datos de carácter personal relativos a la comisión de infracciones penales o administrativas, continua diciendo el citado articulo 7 que: *'… sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras'*. Por tanto la empresa no puede crear o tratar ficheros con esta información.

En las empresas de transporte suele ser una práctica habitual mantener un fichero en el que se registran las multas de tráfico de los conductores de la plantilla.

Debe tenerse en cuenta que una multa de tráfico tiene el carácter de sanción administrativa y por tanto este fichero está prohibido por el citado artículo 7 de la LOPD.

1.2.3. Comunicación, cesión o acceso por terceros.

Se entiende por comunicación de datos toda revelación de datos realizada a una persona distinta del interesado.

De acuerdo con el artículo 11 de la Ley: *'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.'*

Es por tanto necesario que, para la comunicación de datos, concurran dos requisitos: el consentimiento previo del interesado y la existencia de una finalidad legítima que exija dicha comunicación.

La comunicación de datos más habitual en las empresas está relacionada con la prestación de ciertos servicios por un tercero, ajeno a la empresa, y para cuya prestación del servicio es imprescindible que la empresa le facilite los datos del afectado.

La prestación de servicios profesionales de asesoría laboral y confección de nóminas, llevanza de contabilidades, asesoramiento fiscal, incluso auditoría de cuentas, son ejemplos de situaciones en las que el prestador del servicio necesita tener acceso a datos que han sido recabados por la empresa y no por él.

De forma similar otros prestadores de servicios como mensajería y transporte o de mantenimiento y servicio postventa necesitan que la empresa les facilite los datos de los clientes para la prestación del servicio.

En todos los casos la tratamiento de los datos por un tercero no exime a ninguna de las dos partes, responsable del fichero y responsable del tratamiento, de la obligación de cumplir con todas las precauciones establecidas por la Ley en relación con el acceso y tratamiento de los datos personales objeto de la cesión y a su eliminación o restitución una vez concluido el servicio que fue causa de la cesión.

El artículo 5 establece la obligación de informar al interesado de, entre otras cosas, quiénes serán los destinatarios de la información.

En el caso de una Pyme que realiza subcontratación de servicios, para cuya prestación debe facilitar datos personales recabados por aquella, tiene la obligación de incluir a estos subcontratistas como destinatarios de la información en el momento de la recogida de los datos del interesado.

Otro tipo de comunicación de los datos personales contemplada por la Ley es la cesión, este tipo de comunicación de datos por la empresa puede ser motivada por la necesidad de cumplir con las obligaciones legales, mercantiles o fiscales que afectan a la empresa o como consecuencia de las actividades propias de su gestión.

En el primer caso se pueden incluir las comunicaciones realizadas a la Administración Tributaria o la Seguridad Social a través de las declaraciones de percepciones y retenciones a los trabajadores y profesionales colaboradores, en concreto el Modelo 190 de Resumen Anual de retenciones a cuenta del Impuesto de la Renta de las Personas Físicas, o los Formularios TC2 y TC3 de percepciones de los trabajadores y otros muchos que cabría citar.

También se pueden encuadrar en este apartado: el Modelo 390 de Resumen Anual de operaciones sujetas al Impuesto sobre el Valor Añadido, o el Modelo 347 del Resumen Anual de Operaciones.

Similares características tienen las cesiones de datos realizadas en cumplimiento de una sentencia de un Juzgado.

En todos estos casos la cesión de datos por la empresa se realiza en cumplimiento de una norma concreta tal como está previsto en el artículo 11-2 de la Ley, por ello no será necesario obtener la previa autorización del afectado tal como lo establece el artículo 25-2 de la misma.

Consideración diferente tienen ante la Ley las cesiones de datos personales que la empresa lleve a cabo fuera del cumplimiento de una disposición legal, tal es el caso de las cesiones de datos realizadas entre empresas vinculadas o la venta de ficheros de datos personales por la empresa.

En ambos casos será necesario haber cumplido con el deber de informar al interesado:

- De todos los destinatarios de los datos recogidos
- De la finalidad que cada uno de los destinatarios pretende dar a dichos datos.
- Si los datos van a ser objeto de comercialización, es necesario obtener la autorización expresa del interesado para dicho comercio.

1.2.4. Almacenamiento y custodia

La empresa podrá mantener los ficheros de datos personales a efectos de archivos históricos siempre que cumpla con lo dispuesto en el artículo 4 de la LOPD:

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

… 9. Serán almacenados de forma que permitan el ejercicio del derecho de acceso por parte del afectado.'

Así pues, la empresa deberá tomar las precauciones adecuadas para:

- Asignar un periodo de vida a sus archivos históricos.
- Destruirlos de forma efectiva una vez se ha cumplido dicho periodo de vida.
- Asegurarse que durante el periodo de vida se atienda informe al interesado de la existencia de tal fichero si así es requerida por aquel.

1.2.5. Destrucción

Tal como establece el citado artículo 4 de la LOPD: *'…6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.'*

La empresa deberá tomar las precauciones adecuadas para que la destrucción de los ficheros de datos personales sea efectiva, de tal modo que no sea posible la recuperación de dichos datos ni siquiera mediante la utilización de técnicas o procedimientos avanzados de recuperación de datos borrados.

En relación con los ficheros informatizados con datos personales, la empresa debe tener presente la existencia de técnicas informáticas avanzadas que permiten la recuperación de ficheros tras repetidos borrados de éstos. Por ello es aconsejable el empleo de programas de borrado efectivo de ficheros que garanticen la no recuperación de estos.

◆ 1.3 Derechos y acciones por parte del interesado

La Ley 15/1999 es especialmente protectora de los derechos de los interesados, siendo numerosos los artículos en los que se hace referencia a ellos. Para una mayor facilidad los hemos reflejado de forma ordenada en cada fase del tratamiento de los datos personales:

Derecho de información

El artículo 5 establece la obligación de informar al interesado, previamente a la recogida de sus datos, sobre:

- Si los datos serán incluidos en un fichero automatizado de datos o serán objeto de tratamiento informático.
- Cuál es la finalidad para la que se recogen tales datos.
- Quiénes serán los destinatarios de la información recogida.
- Si la respuesta del interesado a las preguntas que les sean planteadas es obligatoria o voluntaria.
- Cuáles son las consecuencias que se derivan de los datos obtenidos.
- Cuáles son las consecuencias que se derivan si se niega a suministrarlos.
- De que en todo momento puede ejercer sus derechos de acceso, rectificación y cancelación.
- Cuál es la identidad y dirección del responsable del fichero.

Consentimiento

El artículo 6 establece el derecho del interesado a dar o negar su consentimiento para que sus datos personales sean tratados informáticamente.

Datos especialmente protegidos

El artículo 7 establece el derecho de las personas a no tener que declarar sobre su ideología, religión o creencias, y la obligación de la empresa a informar al interesado sobre tal derecho.

Cesión

El artículo 11 establece el derecho del interesado a autorizar con carácter previo a cualquier cesión de sus datos, no obligatoria por ley.

Impugnación

El artículo 12 concede al interesado el derecho a impugnar cualquier valoración de su comportamiento cuando ésta se base excluidamente en el tratamiento informatizado de sus datos personales.

Consulta

El artículo 13 permite al interesado la realización de consultas al Registro General de Protección de Datos sobre la existencia de ficheros de carácter personal, su finalidad y la identidad de los responsables de tales ficheros.

Derecho a Indemnización

El artículo 17 de la Ley contempla la posibilidad de que el afectado que resulte perjudicado en sus bienes o derechos, como consecuencia de un incumplimiento de la Ley, pueda pedir indemnización por sus daños al responsable del fichero. Dicha demanda se realizará por la vía civil.

Además de los citados derechos del interesado, por su importancia y efectos para la empresa en caso de no atenderlos son de especial interés los siguientes derechos que también puede ejercer el interesado:

Derecho de acceso

De conformidad con el artículo 15 de la Ley:

'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.'

Es por tanto obligación de la empresa atender a las solicitudes de los interesados, de lo contrario podía incurrir en una infracción muy grave, de acuerdo con el artículo 44.h de esta Ley.

Para cumplir con dicha obligación la Pyme deberá remitir un escrito de contestación al interesado, en el plazo de un mes desde la recepción de la solicitud, informándole de que ha recibido la solicitud y de si ésta se ajusta a derecho y va a ser atendida, o por el contrario presenta defectos o deficiencias (datos incompletos del afectado, ausencia de la copia del D.N.I de éste, etc.) y por ello debe de ser presentada de nuevo con las oportunas rectificaciones.

En el caso de que la petición del interesado se ajuste a derecho, la empresa deberá de remitirle la información solicitada en el plazo máximo de diez días hábiles a contar desde el escrito de acuse de recibo de la solicitud.

El interesado tan solo podrá ejercer este derecho sobre un mismo fichero una vez al año como máximo, salvo causas excepcionales que justifiquen una mayor frecuencia.

Derecho de rectificación y cancelación

El artículo 16 de la Ley establece:

'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.'

De acuerdo con lo dispuesto por la Ley, la Pyme deberá de modificar en el plazo máximo de diez días desde la recepción de la solicitud aquellos datos que el interesado le indique que deben de ser actualizados. Del mismo modo deberá de comunicar dichas modificaciones al responsable del tratamiento, si existe.

De igual modo y plazo deberá de actuar en el caso de que la solicitud del interesado se refiera a la cancelación de sus datos, si bien en este caso se deberán de tener en cuenta las limitaciones legales, contables, fiscales, etc., que obligan a la retención y conservación de los datos por un período determinado. Hasta la conclusión de dicho periodo, la Pyme deberá poner un cuidado especial en que los datos cuya cancelación ha sido solicitada no sean utilizados con ninguna finalidad comercial, publicitaria, informativa o de correspondencia.

En relación con la rectificación y cancelación de datos, hay que tener un especial cuidado con los ficheros o copias de ellos en propiedad de determinados miembros de la empresa o de colaboradores de ésta, (comerciales, personal de mantenimiento, transportistas, etc.). La existencia de tales ficheros en ordenadores portátiles, PDAs, CDs, memorias móviles u otros soportes diferentes de los servidores de la empresa, podrían ocasionar que la información no se actualizase por igual en dichos ficheros, los que podría suponer un incumplimiento leve de la Ley, según el artículo 44-2. Además de otras infracciones adicionales por existencia de ficheros, o de responsables de tratamiento, no declarados.

◆ 1.4 Incumplimiento de la Ley.

Se considera infracción cualquier incumplimiento de la Ley por parte del responsable del fichero o del responsable del tratamiento, ya sea éste por acciones contrarias a las permitidas o por omisión en el cumplimiento de las obligaciones establecidas por esta.

A los efectos de la Ley, el responsable del fichero será la propia empresa a través de su representante legal. En cuanto al responsable de tratamiento, será el tercero que preste dicho servicio a la empresa, si éste existe.

Las empresas que tratan directamente sus datos serán consideradas a la vez responsables del fichero y del tratamiento.

1.4.1. Tipos de infracción

De acuerdo con el artículo 44 de la Ley, las infracciones se califican en tres niveles: leves, graves y muy graves.

Se consideran infracciones leves:

• La falta de atención a la solicitud formulada procedentemente por el interesado sobre la rectificación o cancelación de sus datos personales.

• No atender a las solicitudes información de la Agencia de Protección de Datos en relación con aspectos no clave de la protección de datos.
• No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando ello no sea constitutivo de infracción grave.
• Recoger datos de carácter personal de los propios afectados sin proporcionarles informarles de sus derechos.
• No cumplir con el deber de secreto establecido en el artículo 10 de esta Ley, salvo que dicho incumplimiento constituya una infracción grave.

Se consideran infracciones graves:
• Crear 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.
• La recogida de datos de carácter personal sin recabar, en los casos en que éste sea preceptivo, el consentimiento expreso de los afectados.
• Tratar los datos de carácter personal o usarlos posteriormente incumpliendo los principios y garantías establecidos en la presente Ley
• Ignorar preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
• Impedir u obstaculizar el ejercicio de los derechos de acceso y oposición del afectado.
• Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando, como consecuencia de ello, resulten afectados los derechos de los interesados o sus allegados.
• Incumplir con el deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos calificados como de nivel medio de seguridad, esto es, los relativos a:

- La comisión de infracciones administrativas o penales,
- Datos de 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.

• Mantener los ficheros locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que establece el Reglamento de Medidas de Seguridad.
• 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.
• Poner impedimentos que obstruyan el ejercicio de la función inspectora.
• No cumplir con la obligación de 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.
• 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.

Por último, se consideran infracciones muy graves:
• La recogida de datos en forma engañosa y fraudulenta.
• Comunicar o ceder datos de carácter personal fuera de los casos en los que estén permitidos.
• Recoger y tratar los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias cuando no medie el consentimiento expreso del afectado;
• Recabar y tratar los datos que hagan referencia al origen racial, a la salud y a la vida sexual de las personas cuando no lo disponga una ley o el afectado no haya consentido expresamente.
• Crear o tratar ficheros 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
• Negarse a 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.
• Transferir de forma temporal o definitiva 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 previa del Director de la Agencia de Protección de Datos.

• 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.
• Incumplir con el deber de guardar secreto sobre los datos de carácter personal que hacen referencia a la ideología, afiliación sindical, religión y creencias o a origen racial, a la salud y a la vida sexual, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
• 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 al interesado de la inclusión de sus datos de carácter personal en un fichero.

1.4.2. Sanciones y prescripción de estas

Como ya hemos indicado en repetidas ocasiones, las responsabilidades por los incumplimientos de la LOPD recaerán sobre el responsable del fichero y/o sobre el encargado del tratamiento, tal y como queda establecido en el artículo 43 de la Ley.

El régimen de sanciones que el artículo 45 de la Ley establece para las infracciones es el siguiente:
• Las infracciones leves serán sancionadas con multa de 600 a 60.000 Euros.
• Las infracciones graves serán sancionadas con multa de 60.000 a 300.000 Euros
• Las infracciones muy graves serán sancionadas con multa de 300.000 a 600.000 Euros.

Dada la cuantía de las sanciones y la cantidad y variedad de infracciones previstas por la propia Ley, resulta innecesario recomendar a los responsables de las empresas, en especial de las Pymes, que extremen su atención y precauciones en el cumplimiento de la LOPD y de los reglamentos e instrucciones que desarrollen su aplicación.

La prescripción temporal de estas sanciones, atendiendo al artículo 47 de la Ley es:

- Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.
- El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

Sin embargo, la empresa debe tener en cuenta que en caso de iniciarse un procedimiento sancionador por la Agencia, bien por denucia de parte o como consecuencia de una inspección,

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

En cuanto a las sanciones impuestas como consecuencia de un procedimiento, el mismo artículo 47 establece que:

- 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.
- 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.

2. Cumplimiento del Reglamento de Medidas de Seguridad del Real Decreto 994/1999

2.1 Ámbito de aplicación

En su artículo 1, el Real Decreto establece que: *'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 ….'*

Del propio texto se deduce que:

1. Las medidas deben ser tanto de carácter técnico como de carácter organizativo, no pudiendo basarse únicamente en unas de ellas el cumplimiento de la Norma.

2. La garantía de seguridad aportada por dichas medidas debe cubrir:
- ficheros automatizados,
- centros de tratamiento,
- locales e instalaciones,
- equipos y programas y
- las personas.

Como podemos apreciar, a diferencia de la LOPD, cuyo ámbito contemplaba cualquier fichero con datos de carácter personal, el Reglamento tan solo es de aplicación a los ficheros automatizados (entiéndase informatizados) con datos de carácter personal.

No obstante, constituye una buena práctica la aplicación, en la medida de lo razonable, de las medidas de seguridad previstas por el Reglamento a aquellos ficheros de datos personales que no estén informatizados.

En los términos de la LOPD se define como fichero 'todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.'

Resulta pues adecuado considerar que el término fichero se refiere tanto a las bases de datos, como a las hojas de cálculo, ficheros de texto, imágenes de documentos o incluso correos electrónicos emitidos y recibidos.

◆ 2.2 Niveles y medidas de seguridad de los ficheros

El artículo 3 del Reglamento se establece que, atendiendo a la información que contienen, los ficheros con datos de carácter personal se clasificarán en tres niveles de seguridad: básico, medio y alto.

2.2.1. Nivel básico

De acuerdo con el artículo 4 del Reglamento, se consideran como ficheros con nivel básico de seguridad todos aquellos que contengan datos de carácter personal.

Recordemos que la LOPD definía datos de carácter personal como cualquier información concerniente a personas físicas identificadas o identificables.

Por tanto, la Pyme deberá de considerar como de nivel básico cualquier fichero informatizado que contenga datos relativos a personas físicas en la cuantía suficiente para permitir su identificación inequívoca.

En general podemos considerar que el fichero es de nivel básico si tan solo contiene el nombre y los apellidos y algunos de los siguientes: el domicilio, el número de D.N.I , número de Seguridad Social, o similar, puesto o cargo que ocupa en la empresa, etc.

Las medidas que el Reglamento establece en su capítulo II para los ficheros de nivel básico son:

1. Elaboración de un Documento de Seguridad. (art. 8)

El responsable del fichero deberá elaborar un documento en el que quede reflejada la política de seguridad para dicho fichero. Este documento será de obligado cumplimiento para cuantos tengan acceso al fichero.

El documento de seguridad deberá contener la siguiente información:

- Ámbito de aplicación y recursos protegidos.
- Medidas, normas y controles a aplicar.
- Funciones y obligaciones del personal.
- Estructura del fichero de datos personales y aplicaciones que lo tratan.
- Procedimientos de notificación, gestión y respuesta ante las incidencias del fichero.
- Procedimientos de copias de seguridad y de recuperación de los datos desde las copias.

Dicho documento de seguridad deberá mantenerse actualizado y se revisará periódicamente para adecuarlo a la realidad del fichero.

2. Descripción de las funciones y obligaciones del personal (art. 9)

- Las funciones y obligaciones del personal que acceda a datos personales y a los sistemas de información estarán claramente definidas y documentadas.
- El responsable del fichero tomará las medidas oportunas para que todo el personal sea conocedor de sus funciones y obligaciones y de los riesgos y consecuencias de sus actos.

3. Creación de un Registro de Incidencias (art. 10)

- El procedimiento y gestión de incidencias contendrá un registro que permita identificar la incidencia y su proceso de notificación y resolución.

4. Identificación y autenticación de los usuarios (art. 11)

- El responsable del fichero establecerá una lista actualizada de usuarios con acceso autorizado al sistema de información.

• También establecerá los procedimientos para la identificación y autenticación de dichos usuarios.
• Si la autenticación es mediante contraseñas, establecerá los procedimientos de notificación y revocación de éstas.
• Las contraseñas deberán cambiarse con la periodicidad que determine el Documento de Seguridad.
• Mientras estén vigentes las contraseñas se almacenarán de forma no inteligible.

5. Control de accesos (art. 12)

• Los usuarios tendrán acceso a aquellos datos y recursos del sistema de información que precisen para sus funciones.
• El responsable del fichero establecerá mecanismos para impedir los accesos no autorizados al sistema de información.
• En la relación de usuarios autorizados constarán sus perfiles de acceso.
• La creación y modificación de los perfiles de acceso solamente podrá ser realizada por el personal específicamente autorizado en el Documento de Seguridad.

6. Gestión de los soportes (art. 13)

Los soportes que contengan datos de carácter personal deberán:
• Estar identificados de forma que sea posible conocer el tipo de información que contienen,
• Estar inventariados,
• Ser almacenados en un lugar con acceso restringido solamente a quienes estén autorizados para ello en el Documento de Seguridad.
La salida de soportes con datos personales fuera de los locales donde se encuentra el fichero, únicamente puede ser autorizada por el responsable del mismo.

7. Copias de respaldo y recuperación (art. 14)

• El responsable del fichero se encargará de definir los procedimientos de realización de copias de seguridad y de la recuperación desde éstas.
• Dichos procedimientos deben garantizar la recuperación de los datos en cualquier momento.
• Deberán realizarse copias de respaldo, al menos, semanalmente.

2.2.2. Nivel medio

En el citado artículo 5 del Reglamento se establece que se consideran con nivel medio de seguridad:

- 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.

- Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo

Por tanto, la Pyme deberá establecer medidas de seguridad de nivel medio para todos aquellos ficheros informatizados en que haya incluido datos sobre infracciones administrativas o penales; por ejemplo los que recojan las infracciones de los empleados, las sentencias judiciales por las que se ordena la retención por la empresa de la nómina o parte de ella.

También se indica en el Reglamento que tienen nivel medio de seguridad los ficheros relacionados con la Hacienda Pública. A falta de una mayor clarificación sobre tales ficheros, la Pyme deberá, por prudencia, considerar como tales las declaraciones de los diferentes impuestos, los escritos, requerimientos, recursos y actas que por vía informática se hayan recibido o creado por la empresa.

En relación con la consideración de nivel medio de los ficheros de servicios financieros, también en ausencia de una mayor clarificación y aplicando el criterio de prudencia, la Pyme puede considerar como tales todos aquellosficheros informatizados con datos de carácter personal, que tengan que ver con bancos, cajas, intermediarios financieros o similares, entre ellos y a modo de ejemplo: cuentas bancarias, depósitos, préstamos y créditos con o sin garantía, avales, inversiones en acciones y bonos, etc.

Con la referencia a los ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, el Reglamento se refiere a los fiche-

ros de solvencia patrimonial y de crédito. El tratamiento de tales ficheros ya fue objeto de regulación a través de la Instrucción 1/1995 de la Agencia de Protección de Datos y ahora el Reglamento ha venido a establecer el nivel de seguridad medio para los ficheros informatizados generados como consecuencia y para dicho tratamiento.

Finalmente el Reglamento establece que deberán tener nivel de seguridad medio aquellos ficheros que contengan datos mediante los cuales sea posible realizar una evaluación de la personalidad del individuo. Tal y como ocurre con los test psicotécnicos, perfiles de comportamiento y otros ficheros similares resultantes de pruebas realizadas por evaluadores y psicólogos dentro de su actividad profesional.

Ante estos ficheros, que con frecuencia forman parte de la documentación generada en el proceso de selección de candidatos, la Pyme debe mantener un alto grado de prudencia y mantenerlos dentro del ámbito de los recursos humanos, bajo las medidas de seguridad establecidas por el Reglamento para el Nivel Medio de Seguridad.

Cabe considerar también dentro de este grupo de ficheros los currículums que de forma voluntaria son remitidos a la Pyme por los interesados, como vía para postular su candidatura a un puesto de trabajo en aquella. En general dichos ficheros son recibidos por distintas vías: correo postal, telefax, correo electrónico, entrega en mano, etc.

Ni el carácter voluntario de la entrega ni la forma en que ha sido recibido eximen a la Pyme de su responsabilidad en cuanto a la protección y seguridad de la documentación recibida, que en todos los casos deberá ser protegida con medidas de nivel medio durante el periodo que dichos historiales permanezcan en poder de la Pyme; y concluido éste aquella deberá asegurarse de que la destrucción de los ficheros fue adecuada.

Las medidas que el Reglamento establece en su capítulo II para los ficheros de nivel medio son:

1. Todas las ya definidas para los ficheros de nivel básico

2. Documento de seguridad ampliado (art. 15)
Además de lo dispuesto para el nivel básico, el Documento de Seguridad deberá contener:

- Identificación del responsable o responsables de seguridad.
- Controles periódicos a realizar para verificar el cumplimiento del mismo.
- Medidas a aplicar en caso de soportes desechados o reutilizados.

3. Responsable de seguridad (art. 16)
El responsable del fichero designara uno o más responsables de seguridad, encargados de coordinar y controlar el cumplimiento de Documento de Seguridad.

La existencia de responsables de seguridad no exime al responsable del fichero de sus responsabilidades.

4. Auditoría (art. 17)
- Los sistemas de información e instalaciones de tratamiento deberán someterse a una auditoría, interna o externa, al menos cada dos años.
- El objeto de la auditoría será verificar el cumplimiento del Reglamento y de los procedimientos e instrucciones recogidos en el Documento de Seguridad.
- El informe pondrá de manifiesto la adecuación de la medidas y controles al Reglamento y la existencia de debilidades de seguridad y la necesidad de medidas o controles complementarios.
- El informe de auditoría se sustentará con hechos y evidencias concretas.
- El informe de auditoría será analizado por el responsable de seguridad, quien a la vista del mismo propondrá al responsable del fichero las medidas a implantar.
- La Agencia de Protección de Datos podrá solicitar los informes de auditoría y verificar la puesta en práctica de las recomendaciones hechas por el responsable de seguridad.

5. Identificación y autenticación (art.18)
El responsable del fichero establecerá los mecanismos de identificación inequívoca del usuario y la verificación de que se encuentra autorizado.

Se limitará la posibilidad de intentos reiterados de acceso no autorizado al sistema de información.

6. Control de acceso físico (art.19)
El acceso a los locales donde se encuentren ubicados los sistemas de información estará restringido a los usuarios autorizados.

7. Gestión de soportes (art.20)
• Deberá establecerse un registro de entrada de soportes que permita identificar su origen y contenido.

• Así mismo deberá establecerse un registro de salida de soportes con similares características al anterior

• Cuando un soporte vaya a ser desechado o reutilizado se tomarán las medidas adecuadas para impedir la recuperación de la información que contenía con anterioridad.

• Cuando los soportes vayan a salir fuera de las instalaciones de los sistemas de información se tomarán las medidas para impedir la recuperación indebida de su contenido.

8. Registro de incidencias (art. 21)
Además de lo establecido para los ficheros de nivel básico, el registro recogerá información sobre los procedimientos de recuperación, la identidad de quién la realizo, los datos restaurados y si fue necesario recurrir a procedimientos de grabación manual.

9. Prohibición de pruebas con datos reales (art. 22)
Las pruebas de nuevos aplicativos o de las modificaciones de los existentes no podrá realizarse en los sistemas de información sobre ficheros con datos reales, salvo que pueda asegurarse el mantenimiento del nivel de seguridad existente.

2.2.3. Nivel alto
El referido artículo 5 del reglamento establece que deberán considerarse como nivel alto de seguridad:

• 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

Resulta comprensible que, con independencia de las limitaciones establecidas por la LOPD en cuanto a la creación y existencia de los ficheros de ideología, religión , creencias o vida sexual y a los de salud, en el caso de que dichos ficheros existan, deberán estar sujetos a las medidas de seguridad del más alto nivel.

Así mismo es lógico considerar como de nivel alto de seguridad a los ficheros resultantes de un proceso de investigación policial, toda vez que dichos datos fueron recabados sin consentimiento de los afectados.

La realización de la Vigilancia de la Salud de los trabajadores da como consecuencia dos tipos de información:

• De una parte un fichero con los resultados de las pruebas médicas realizadas al trabajador, generalmente por la Mutua, que suele quedar en poder de ésta. Dicho informe contiene datos de salud, y por tanto debe ser considerado de Nivel Alto, siendo responsabilidad de la Mutua establecer dichas medidas.
En cuanto a la responsabilidad del fichero a efectos de su inscripción en el Registro de la Agencia de Protección de datos, la práctica habitual es que sea la Mutua quien lo inscriba como fichero propio. De no hacerlo así, debe ser la Pyme quien lo inscriba como propio, designando como 'Encargado del tratamiento' a la Mutua.

• De la otra parte, el informe sobre la situación del trabajador, en el cual tan solo aparece la calificación de 'apto' o 'no apto' para el desempeño de su trabajo, tiene carácter de fichero de datos personales.

Nivel alto son:

1. Todas las ya definidas para los ficheros de nivel básico y medio.

2. Distribución de soportes. (art. 23)

La distribución de soportes que contengan ficheros de datos de carácter personal de nivel alto se realizará cifrando dichos datos o bien utilizando mecanismos que garanticen que dichos datos resultan ininteligibles.

3. Registro de accesos. (art. 24)
El responsable del fichero deberá establecer un registro en el que se conserve de cada acceso al menos:
- Identificación del usuario.
- Fecha y hora del acceso
- Fichero accedido
- Tipo de acceso
- Si ha sido autorizado o denegado.
- En caso de acceso autorizado, información del registro accedido.

Este registro estará bajo el control de responsable de seguridad, que deberá investigar los intentos de acceso denegados.

Se deberán conservar los registros de acceso al menos durante dos años.

El responsable de seguridad elaborará un informe mensual de los controles y revisiones realizados.

4. Copias de respaldo y recuperación. (art. 25)
Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentran los sistemas informáticos que los tratan.

Dicho lugar deberá cumplir con las medidas de seguridad establecidas por el Reglamento para los datos de nivel alto.

5. Telecomunicaciones. (art. 26)
La transmisión de los datos de nivel alto a través de redes de comunicaciones se realizará cifrando éstos o utilizando cualquier otro medio que garantice que resultan ilegibles.

◆ 2.3 Incumplimientos del Reglamento de Medidas de Seguridad

El incumplimiento por la Pyme de las medidas de seguridad establecidas en el reglamento para los ficheros de titularidad privada será sancionado de acuerdo con lo establecido en el artículo 42 de la Ley 15/1999.

La responsabilidad de las infracciones recae sobre el responsable del fichero y sobre el encargado del tratamiento, en su caso, de acuerdo con lo establecido en citado artículo.

2.3.1. Tipos de Infracciones

Según el artículo 44 -3-h de la LOPD se considera infracción grave: *'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'.*

Por tanto, cualquier incumplimiento de las medidas de seguridad establecidas por el Reglamento tiene la consideración de infracción muy grave.

2.3.2. Sanciones

De acuerdo con lo establecido en el artículo 45 de la Ley 15/1999, las infracciones graves se sancionarán con multas de 60.000E a 300.000E.

Como el citado artículo 45 establece, en la graduación de la cuantía de las sanciones se tendrán en cuenta la naturaleza de los derechos personales afectados, el volumen de los tratamientos efectuados, los beneficios obtenidos, el grado de intencionalidad, la reincidencia, los daños y perjuicios causados a las personas interesadas y las terceras personas, y cualquier otra circunstancia que sea relevante para determinar el grado de intencionalidad y de culpabilidad presentes en la concreta actuación infractora.

◆ 2.4 Plazos para la implantación de las Medidas de Seguridad.

Según establecía la Disposición Transitoria Única del Real Decreto, las medidas de seguridad de nivel básico debían implantarse en el plazo de seis meses a partir de la entrada en vigor del Reglamento, para la medidas de nivel medio se concedía un año y para las de nivel alto dos años.

Excepcionalmente se concedía un plazo de tres años para la implantación de las medidas de seguridad en aquellos sistemas que presentasen dificultades tecnológicas para la implantación de alguna de estas.

Teniendo en cuenta la publicación del Real Decreto 994 en el B.O.E. número 151 del 25 de Junio de 1999, los plazos deberían haber sido:

Medidas	Fecha límite de implantación
Nivel básico	25 de Diciembre de 1999
Nivel medio	25 de Junio de 2000
Nivel alto	25 de Junio de 2001
Sistemas con dificultades tecnológicas	25 de Junio de 2002

La promulgación de la Ley 15/1999 en el B.O.E. número 298 del 14 de diciembre de 1999 modificó dichos plazos, ampliando la fecha límite de la implantación de las medidas de nivel básico hasta el 25 de marzo de 2000.

Con posterioridad y con motivo de las modificaciones establecidas en algunos sistemas de información como consecuencia del llamado 'Efecto 2000', se amplió un año la entrada en vigor de las medidas de seguridad de nivel medio, quedando fijada la fecha límite en el 25 de junio de 2001.

Hasta la fecha de esta publicación no se han producido nuevas ampliaciones ni modificaciones de plazos, por lo que las empresas, incluidas las Pymes, deberían tener ya implantadas todas las medidas de seguridad correspondientes a los tres niveles.

3. La Agencia de Protección de Datos

3.1 Origen

El artículo 34 de la Ley 5/1992 establece la creación de la Agencia de Protección de Datos como un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, independiente en sus actuaciones de las Administraciones Públicas y dotada para su funcionamiento de un estatuto propio.

El Real Decreto 428/1993 de 26 de marzo aprobaba el estatuto de la Agencia de Protección de Datos.

La Ley 15/1999, en su artículo Título IV, ratifica y amplía las funciones y capacidades de la Agencia, siendo estas las actuales.

3.2 Funciones

De conformidad con lo establecidos por el artículo 37 de la Ley 15/1999, 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.

Las citadas funciones podemos agruparlas a efectos prácticos en tres grupos:

1. Registro y control de los ficheros con datos personales.
Es función de la agencia mantener el Registro de General de Protección de Datos.

De acuerdo con lo establecido en el artículo 39 de la Ley 15/1999, serán objeto de inscripción en el Registro General de Protección de Datos:
- Los ficheros de los que sean titulares las Administraciones públicas.
- Los ficheros de titularidad privada.
- Las autorizaciones a los que se refiere la presente Ley.
- Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

Además, el artículo 26 de la citada Ley, establece:

'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. 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.

3. 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.

4. 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.'

A la vista de ambos artículos queda clara la línea de actuación que debe seguir la Pyme en el proceso de creación e inscripción de sus ficheros de datos personales en el Registro:

a. Para los ficheros ya existentes, solicitud de su inscripción en el registro.

b. Para los ficheros de datos personales que necesite crear en el futuro, notificación a la Agencia de Protección de Datos, previa a la creación del fichero.

2. Autorización de los movimientos internacionales de datos.
El artículo 33 de la LOPD establece que:
'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.'

Por tanto corresponde al Director de la Agencia autorizar de forma específica la transferencia internacional de datos personales.

No parece que sea una práctica habitual en la Pyme el envío de datos personales a otros países. Pero es práctica habitual el remitir a los corresponsales, agentes o delegados de la empresa en otros países la relación de contactos o clientes de ese país a los que se ha recibido y atendido con motivo de una feria, una exposición o un congreso. En función de la información remitida, dicho envío tendría el carácter de movimiento internacional de datos.

3. Atención a consultas.
La Agencia de Protección de Datos dispone los medios para la atención de las consultas formuladas por los ciudadanos y empresas en relación con la aplicación de la Normativa de Protección de Datos.

Las consultas pueden ser formuladas por correo, teléfono, telefax o a través de de la página Web de la Agencia .

La Memoria de la Agencia correspondiente al año 2002, publicada en septiembre de 2003, presenta los siguientes datos em relación con las consultas atendidas por durante el ejercicio 2002:

Consultas formuladas por las Administraciones Públicas	199
Consulta formuladas por particulares y empresas	216

De las 415 consultas recibidas, 180 fueron relativas a cesión de datos y 80 estaban relacionadas con el consentimiento del afectado, curiosamente menos del 5% de las preguntas totales tenían que ver con datos protegidos.

4. Realización de inspecciones.
El artículo 40 de la Ley 15/1999 atribuye a la Agencia la función de inspección al manifestar que:

'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.'

Las actuaciones inspectoras de la Agencia son de dos tipos:

a. Actuaciones sujetas a un Plan de Inspección.

b. Actuaciones motivadas por denuncias de los afectados.

Los Planes de inspección sectoriales de mayor impacto llevados a cabo por la Agencia a lo largo de los últimos años han sido:

- Plan de inspección de los Hospitales Públicos en 1995 y 1996
- Plan sectorial de inspección de salas de Bingo en 1998
- Plan de inspección de los ficheros de la Dirección General de Tráfico en 1999
- Plan de inspección de Grandes Superficies Comerciales en el año 2000
- Plan de inspección de Banca a Distancia en el 2001
- Plan de inspección de los ficheros de Solvencia Patrimonial y de Crédito en el 2001
- Plan de inspección de Seguros de Automóvil en el 2001
- Plan de inspección de la Cadenas Hoteleras durante los años 2002 y 2003
- Plan de inspección de Empresas de Comercio Electrónico en el 2002

En cuanto a la oportunidad y calidad de las acciones inspectoras, de la citada Memoria del 2002, extraemos las siguientes cifras:

- 99 Sentencias de los Tribunales Superiores de Justicia en relación con recursos contra inspecciones de la Agencia de Protección de Datos.
    - 79 Desestimaron el recurso en su totalidad.
    - 10 Desestimaron parcialmente el recurso
    - 10 Anularon las actuaciones de la inspección.
- 11 Sentencias del tribunal Supremo en relación con recursos contra inspecciones de la Agencia de Protección de Datos.
    - 8 Estimaron que no ha lugar el recurso.
    - 3 Estimaron que el recurso era procedente.

4. Pasos a seguir para adaptarse a la Normativa

La empresa puede adaptar sus sistemas de información a la Normativa de Protección de Datos mediante una serie de etapas que no deberían de suponer entorpecimiento en su actividad cotidiana. El programa de adaptación deberá contemplar los siguientes pasos:

Identificar los ficheros con datos de carácter personal.
La empresa deberá elaborar un inventario de los ficheros que posee y gestiona, con independencia de cual sea su suporte, papel o electrónico. Dicho inventario debería contener información sobre:

- responsable funcional del fichero,
- departamento y soporte en que se encuentra,
- personas o aplicaciones que tienen acceso a este fichero.
- tipo de datos que contiene y estructura del fichero.
- origen de los datos que contiene.
- forma en que se obtuvieron.
- ubicaciones alternativas, copias, etc.
- cesiones, cesionarios y disposición que las permite.
- accesos por terceras personas.
- si se realiza transferencia internacional del fichero, países de destino y autorizaciones para ello.

Notificar los ficheros con datos personales a la Agencia de Protección de Datos.
Aquellos ficheros inventariados que contengan datos de carácter personal deben ser comunicados a la Agencia, para ello se pueden utilizar los formularios de notificación facilitados por ésta a través de su página web.

La comunicación de los ficheros de datos personales a la Agencia se debe realizar tan pronto como los ficheros son identificados, cuando se

haya producido alguna modificación en la estructura de alguno de los ficheros declarados previamente o cuando se cree un nuevo fichero de datos personales.

Designar las funciones de responsable de seguridad (si existen ficheros de nivel medio o alto).

La función de responsable de seguridad puede ser asignada a una o a varias personas, en función del número de ficheros con datos personales, su ubicación y el tipo de gestión que se realiza sobre ellos, la empresa determinará el número más adecuado de responsables.

Los responsables de seguridad que estén en tales funciones deben aparecer reflejados en el Documento de Seguridad de cada fichero y deberán realizar las tareas que les han sido atribuidas por responsable del fichero.

Identificar los riesgos de seguridad que pueden afectar a cada fichero.

Cada fichero de datos personales está sujeto a una serie de riesgos de seguridad como consecuencia de los diferentes tratamientos a que se encuentra sometido. La empresa debe evaluar dichos riesgos e identificar las medidas de seguridad más adecuadas para reducir dichos riesgos al mínimo.

El resultado del análisis de riesgos y medidas de seguridad será tenido en cuenta para la confección de Documento de Seguridad de cada fichero.

Elaborar el Documento de Seguridad para cada fichero o grupo de ficheros de un mismo nivel de seguridad.

Como hemos visto, la estructura y contenido del Documento de Seguridad es un requisito del Reglamento de Medidas de Seguridad (Ver art. 8 y 15 del Reglamento).

El Documento de Seguridad puede ser elaborado de forma individual para cada fichero o bien incluir en un mismo Documento de Seguridad un grupo de ficheros con el mismo nivel de seguridad y cuyas características y gestión sean similares.

El responsable del fichero deberá conservar y mantener actualizado el Documento de Seguridad y facilitárselo a la Agencia de Protección de Datos en caso de que ésta lo requiera durante el proceso de una inspección.

Poner en la práctica los procedimientos y medidas descritos en cada Documento de Seguridad.

Los procedimientos descritos en el Documento de Seguridad, los controles identificados en él y las demás medidas que en éste se describan para asegurar la información contenida en el fichero deben ser aplicados en el plazo más breve, con el fin de minimizar los riesgos sobre el fichero.

En ocasiones la puesta en práctica de los procedimientos requerirá de la adquisición e instalación de ciertos medios de seguridad: Software de antivirus, firewalls, software de control de accesos, etc., en cuyo caso es conveniente que dicha instalación sea realizada por especialistas.

Sin embargo, la mayoría de los procedimientos y controles afectarán a los usuarios del fichero, por lo que es imprescindible que éstos reciban una formación adecuada.

La formación de los usuarios deberá contemplar:

- obligaciones y funciones que les afectan por acceder a datos de carácter personal,
- conocimiento de los riesgos que afectan a los ficheros de datos personales,
- procedimientos y controles establecidos para minimizar dichos riesgos,
- operaciones a realizar en caso de detectar una incidencia en un fichero de datos personales.

El responsable del fichero deberá conservar constancia de la acción formativa realizada y de los resultados de dicha formación: calificaciones de los asistentes, valoraciones de los mismos, etc.

Revisar los incidentes de seguridad, analizar sus causas y aplicar las medidas correctoras precisas.

El Registro de Incidencias que establece el Artículo 10 del Real Decreto debe ser revisado de forma regular por el responsable del fichero con el

fin de verificar que todas las incidencias reflejadas en él se encuentran cerradas o en vías de solución y no existen por tanto incidencias abiertas con una antigüedad excesiva.

La revisión del Registro de Incidencias deberá poner de manifiesto aquellas incidencias que son recurrentes y por tanto es conveniente iniciar una acción correctiva que suprima las causas de dicha recurrencia.

Si como consecuencia de estas acciones correctivas fuera necesario modificar algún procedimiento o bien establecer nuevos controles sobre el fichero, este hecho debería ser trasladado al Documento de Seguridad del fichero.

Auditar el funcionamiento de las medidas establecidas en cada Documento de Seguridad.

La obligación de auditar, al menos cada dos años, el cumplimiento del Reglamento de Medidas para las empresas que tienen ficheros de datos personales de nivel medio o alto viene establecido en el artículo 17 del Real Decreto.

La auditoría puede ser realizada por profesionales externos a la empresa o bien por el propio personal de ésta, siempre que dicho personal posea los conocimientos adecuados sobre la Normativa de Protección de Datos y sea independiente de los ficheros y procedimientos auditados.

Aunque la frecuencia obligatoria de las auditorías es bianual, constituye una buena práctica la realización de auditorías de menor alcance y con una mayor frecuencia, digamos semestralmente, de forma que cada dos años se haya realizado la auditoría de todos los ficheros y procedimientos de la empresa.

La realización de auditorías más frecuentes permite que las deficiencias de seguridad detectadas en ficheros, procedimientos, medidas o controles sean corregidas en un menos plazo, reduciéndose así los riesgos de que estas deficiencias pudieran ser explotadas por un tercero.

5. Glosario de términos

Accesos autorizados	Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. (R.D. 994 Art. 2)
Afectado o interesado	Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo. (LOPD. Art. 3)
Autenticación	Procedimiento de comprobación de la identidad de un usuario. (R.D. 994 Art. 2)
Control de acceso	Mecanismo que en función a la identificación ya autenticada permite acceder a datos o recursos. (R.D. 994 Art. 2)
Cesión o comunicación de datos	Toda revelación de datos realizada a una persona distinta del interesado. (LOPD. Art. 3)
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. (LOPD. Art. 3)
Contraseña	Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario. (R.D. 994 Art. 2)
Copia de respaldo	Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación. (R.D. 994 Art. 2)
Datos de carácter personal	Cualquier información concerniente a personas físicas identificadas o identificables. (LOPD. Art. 3)

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. (LOPD. Art. 3)
Fichero	Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. (LOPD. Art. 3)
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. (LOPD. Art. 3)
Incidencia	Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos. (R.D. 994 Art. 2)
Identificación	Procedimiento de reconocimiento de la identidad de un usuario. (R.D. 994 Art. 2)
Procedimiento de disociación	Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable. (LOPD. Art. 3)
Recurso	Cualquier parte componente de un sistema de información. (R.D. 994 Art. 2)
Responsable de seguridad	Persona o personas de la organización a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables. (R.D. 994 Art. 2)

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. (LOPD. Art. 3)
Sistema de información	Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacena miento y tratamiento de datos de carácter personal. (R.D. 994 Art. 2)
Soporte	Objeto físico susceptible de ser tratado en un sistema de información sobre el cual se pueden grabar o recuperar datos. (R.D. 994 Art. 2)
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. (LOPD. Art. 3)
Usuario	Sujeto o proceso autorizado para acceder a datos o recursos. (R.D. 994 Art. 2)

Anexos

Anexo I

Modelo de estructura de un Documento de Seguridad de un Fichero

I. Ambito De Aplicación

I.1. Ambito Jurídico
I.2 Ambito Personal
I.3 Ambito Material

II. Medidas De Seguridad

II. 1. Acceso A Datos A Través De Redes De Comunicaciones
II. 2. Régimen De Trabajo Fuera De Los Locales De La Ubicación Del Fichero
II. 3. Ficheros Temporales
II.4. Identificación Y Autenticación
II.5. Control De Acceso
II 6. Gestión De Soportes
II.7. Auditoría
II. 8. Control De Acceso Físico
II. 9. Pruebas Con Datos Reales
II. 10. Uso Del Correo Electrónico
II. 11. Acceso A Internet
II. 12. Propiedad Intelectual E Industrial
II. 13. Uso De Portátiles
II. 14. Gestión De Papeleras

III. Funciones Y Obligaciones Del Personal

III . 1. Obligaciones De Todo El Personal
III.1.1. Códigos De Identificación Y Claves De Acceso
III.1.2. Confidencialidad De La Información

Modelo de Registro de Incidencias

Incidencia en Fichero de Nivel medio y alto						
Incidencia en fichero de nivel básico						
Número	Fecha/Hora	Descripción de la Incidencia	Hora de concurrencia	Informante	Notificada a	

Anexo II

Daños ocasionados	Método de recuperación de datos	Recuperación realizada por	Grabación Manual S/N	Autorizante de recuperación desde copia	Documento de autorización

Modelo de Registro de Entrada/Salida de Soportes

Número	Entrada/Salida	Fecha y Hora	Procedencia/ Destino	Tipo de soporte	Número de soportes

Anexo III

Tipo de Información contenida	Forma de envío	Receptor/ Emisor	Número de autorización

Anexo IV

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

JUAN CARLOS I
REY DE ESPAÑA

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

Título I. Disposiciones generales

Artículo 1. Objeto.
La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

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

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

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

b. Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
c. Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:
a. A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b. A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c. A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:
a. Los ficheros regulados por la legislación de régimen electoral.
b. Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
c. Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
d. Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
e. Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. Definiciones.

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

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

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

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

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

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

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

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

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

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

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

grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

Título II. Principios de la protección de datos

Artículo 4. Calidad de los datos.

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

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

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

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

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.
No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

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

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

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

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

f. 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.

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

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

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

j. 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 inequí-

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

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

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

Artículo 6. Consentimiento del afectado.

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

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

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

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

Artículo 7. Datos especialmente protegidos.
1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.
Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

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

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

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

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

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

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

Artículo 8. Datos relativos a la salud.
Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. Seguridad de los datos.
1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

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

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

Artículo 10. Deber de secreto.
El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos.
1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:
   a. Cuando la cesión está autorizada en una ley.
   b. Cuando se trate de datos recogidos de fuentes accesibles al público.
   c. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
   d. Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e. Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

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

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

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

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

Artículo 12. Acceso a los datos por cuenta de terceros.
1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

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

se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

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

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

Título III. Derechos de las personas

Artículo 13. Impugnación de valoraciones.
1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

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

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

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

Artículo 14. Derecho de consulta al Registro General de Protección de Datos.
Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho de acceso.
1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

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

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

Artículo 16. Derecho de rectificación y cancelación.
1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

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

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

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

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

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

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

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

Artículo 18. Tutela de los derechos.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

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

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

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

Artículo 19. Derecho a indemnización.
1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

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

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

Título IV. Disposiciones sectoriales

Capítulo I. Ficheros de titularidad pública

Artículo 20. Creación, modificación o supresión.
1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:
   a. La finalidad del fichero y los usos previstos para el mismo.
   b. Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
   c. El procedimiento de recogida de los datos de carácter personal.
   d. La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
   e. Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
   f. Los órganos de las Administraciones responsables del fichero.
   g. Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
   h. Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

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

Artículo 21. Comunicación de datos entre Administraciones públicas.
1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

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

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

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

Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.
1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser

almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

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

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

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

Artículo 23.
Excepciones a los derechos de acceso, rectificación y cancelación.
1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

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

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del

organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. Otras excepciones a los derechos de los afectados.
1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

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

Capítulo II. Ficheros de titularidad privada

Artículo 25. Creación.
Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. Notificación e inscripción registral.
1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figura-

rán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

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

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.
En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

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

Artículo 27. Comunicación de la cesión de datos.
1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

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

Artículo 28. Datos incluidos en las fuentes de acceso público.
1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.
Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.
La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.
En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

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

Artículo 29. Prestación de servicios de información sobre solvencia patrimonial y crédito.
1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho

registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

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

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

Artículo 30.
Tratamientos con fines de publicidad y de prospección comercial.
1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

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

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

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

Artículo 31. Censo promocional.
1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

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

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

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

Artículo 32. Códigos tipo.
1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.
En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

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

Título V. Movimiento internacional de datos

Artículo 33. Norma general.

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

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

Artículo 34. Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación:

a. Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

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

Título VI. Agencia de Protección de Datos

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a. Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b. Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c. Cualesquiera otros que legalmente puedan serle atribuidos.

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

Artículo 36. El Director.

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.
En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. Funciones.

Son funciones de la Agencia de Protección de Datos:

a. Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b. Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c. Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d. Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e. Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f. Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g. Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h. Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.
i. Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
j. Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.
k. Redactar una memoria anual y remitirla al Ministerio de Justicia.
l. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como des empeñar 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.

Disposiciones adicionales, transitorias, derogatoria y finales

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 V

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

El artículo 18.4 de la Constitución Española establece que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, prevé en su artículo 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas 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 que estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el artículo 43.3 h) que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por via reglamentaria se determinen constituye infracción grave en los términos previstos en la propia ley.

Sin embargo, la falta de desarrollo reglamentario ha impedido disponer de un marco de referencia para que los responsables promovieran las adecuadas medidas de seguridad y, en consecuencia, ha determinado la imposibilidad de hacer cumplir uno de los más importantes principios de la Ley Orgánica.

El presente Reglamento tiene por objeto el desarrollo de lo dispuesto en los artículos 9 y 43.3. h) de la Ley Orgánica 5/1992. El Reglamento

determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor.

En su virtud, a propuesta de la Ministra de Justicia, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 11 de junio de 1999.

DISPONGO

Artículo único. Aprobación del Reglamento

Se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, cuyo texto se inserta a continuación.

Disposición final única. Entrada en vigor

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado"

Dado en Madrid a 11 de junio de 1999.

JUAN CARLOS R.

Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal

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 de 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 sobre el cual se pueden grabar o recuperar datos.

11.Responsable de seguridad: Persona o personas de la organización 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 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 en el sistema de información o en la organización.

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 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 los derechos de acceso autorizados 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 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 deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

3.Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

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 articulo 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 personalizado 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 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 v 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 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 periodo 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 del fichero, 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.
Competencia 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.

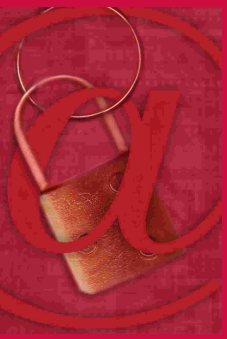
2.Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se cumplan las medidas de seguridad previstas en el presente Reglamento.

Disposición transitoria

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.



Protección de datos y PYMES

anetcom

C/ Luis Vives 6, 4º, 12º
46003 Valencia
Tel. 96 392 39 16
Fax 96 392 40 83
informacion@anetcom.es
www.anetcom.es

GENERALITAT VALENCIANA
CONSELLERIA D'EMPRESA, UNIVERSITAT I CIÈNCIA