Guía para el cumplimiento de la Ley Orgánica de Protección de Datos en una pequeña empresa sin departamento de informática

Realizado por: Sandra González Muñoz

Dirigido por: Dr. D. Juan Vicente Oltra

Escuela Técnica Superior de Ingeniería Informática etsinf

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

ÍNDICE:

Objeto y objetivos del proyecto 4

Introducción 5

Sistemas de Información y Tecnologías de la Información 6

Ley Orgánica de Protección de Datos de Carácter Personal: la LOPD 8

Antecedente a la LOPD: LORTAD 11

Cuestionario de adecuación de la LOPD 12

Análisis de la LOPD 13
- Objeto 13
- Ámbito de aplicación 13
- Calidad de los datos 15
- Derecho de información en la recogida de datos 16
- Consentimiento para el tratamiento de los datos 18
  - Consentimiento para el tratamiento de datos de menores de edad 19
- Revocación para el tratamiento de los datos 19
- Datos especialmente protegidos y datos relativos a la salud 20
- Seguridad en los datos 21
- Deber de secreto 21
- Comunicación o cesión de los datos 22
- Acceso a los datos por cuenta de terceros 22
- Derechos de las personas 24
  - Ejercitación de los derechos 24
  - Procedimiento de ejercer esos derechos 25
  - Derecho de consulta al Registro General de Protección de Datos 25
  - Derecho de impugnación de valores 26
  - Derecho de acceso 26
  - Derecho de rectificación y cancelación 27
  - Derecho de oposición 28
  - Tutela de los derechos 28
  - Derecho a indemnización 29
- Ficheros de titularidad pública y ficheros de titularidad privada 29
- Inscripción de ficheros 30
- Ficheros Temporales 32
- Movimiento internacional de datos 33
- Agencia de Protección de Datos 34
- Infracciones y sanciones 36
  - Infracciones leves 37
  - Infracciones graves 37
  - Infracciones muy graves 38
  - Sanciones 39

Documento de Seguridad 40
- Medidas de seguridad 40

Nivel básico 40
Nivel medio 40
Nivel alto 41
Documento de seguridad 41
Funciones y obligaciones del personal 43
Normas y procedimientos de seguridad 44
Identificación y autenticación 45
Control de acceso 46
Gestión de cuentas servicios y contraseñas 49
Gestión de soportes 50
Acceso a datos a través de redes de comunicaciones 52
Régimen de trabajo fuera de los locales de la ubicación del fichero 52
Ficheros temporales 53
Copias de seguridad 53
Restauración copias de seguridad 55
Gestión de incidencias 56
Auditoría 57
Pruebas con datos reales 58
Controles periódicos 59
Revisión del Documento de Seguridad 59

Tratamiento de datos en el ámbito de Internet 61
Ley de Servicios de la Sociedad de Información y de Comercio Electrónico (LSSI) 61

Conclusiones 64

Bibliografía 65

Glosario 67

Anexos 70

OBJECTO Y OBJECTIVOS DEL PROYECTO:

El objeto del presente Proyecto Fin de Carrera es la obtención del título de Ingeniero en Informática expedido por la Universidad Politécnica de Valencia.

El objetivo de dicho proyecto es la creación de una guía para el cumplimiento de la Ley Orgánica de Protección de Datos en una pequeña empresa sin departamento de informática.
Tras la puesta en vigor de la Ley Orgánica de Protección de Datos (LOPD), son muchas las empresas que se han visto afectadas por esta ley y las cuales están obligadas a garantizar el derecho fundamental a la protección de datos si trabajan con ficheros que contienen datos personales. A partir de ese momento, muchas otras empresas se crearon con el fin de estudiar con detenimiento esta ley y poder crear guías y normativas y poder ofrecer servicios de asesoramiento a otras. De modo que existen en el mercado otras muchas guías como la que vamos a elaborar, pero con la diferencia de que ésta pretende acercar a las pequeñas empresas españolas sin departamento de informática, de forma fácil y sencilla, el contenido de la normativa de la LOPD que está tomando gran importancia en estos últimos años. Recalcar que cuando hablamos de pequeñas empresas nos referimos a empresas con dos o tres operarios. Decir también que el cumplimiento de la LOPD es el mismo para todas las empresas sin distinción según el tamaño ni la facturación o el sector de la actividad.

Nos dirigimos específicamente a este tipo de empresas ya que las pymes y micropymes constituyen más del 99% del sector empresarial español y son el motor principal de la economía y de la generación del empleo en España.

Otro motivo de la creación de esta guía es el hecho de que las empresas grandes fueron las primeras en adecuarse a la LOPD y son las medianas y las pequeñas las que todavía están en fase de adopción e implementación. Esto es debido a la reducida disponibilidad de recursos técnicos, económicos y humanos específicos en seguridad con los que cuentan las pequeñas empresas.

Esta guía recoge los principales aspectos que han de tener en cuenta este tipo de empresas a la hora de tratar los datos de carácter personal tanto de sus clientes, como de sus proveedores y como de su personal empleado entre otros, de modo que ofrece unas pautas para la adaptación a esta ley.
Además, se recogen las disposiciones y obligaciones que afectan a la empresa así como los beneficios para el negocio que se derivan de su adopción.

Si usted posee o forma parte de una pequeña empresa sin departamento de informática, debe cumplir esta guía con exactitud a fin de evitar sanciones por parte de la Agencia Española de Protección de Datos.

Por último, simplemente recordar que hay un principio básico del Derecho que dice: "*el desconocimiento de la Ley no exime de su cumplimiento".*

INTRODUCCIÓN:

En el primer apartado de esta guía encontrará una breve introducción a los Sistemas de Información y Tecnologías de la Información, para que pueda comprobar la gran necesidad de integración entre estos sistemas y tecnologías y las empresas hoy en día.

En los tres apartados siguientes se expondrá qué es la Ley Orgánica de Protección de Datos, el porqué de su surgimiento, la ley que le precedía (LORTAD) y las diferencias entre ambas.

En el cuarto apartado de la guía se le presentará el marco legal específico que regula la protección de datos. Se analizará en este capítulo todos los artículos de la LOPD para que usted pueda entender el funcionamiento de ésta y se darán pautas de comportamiento para poder aplicarlas en su lugar de trabajo.

A continuación, en el quinto apartado se tratará el Documento de Seguridad en el que se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Para ampliar sus conocimientos en temas de protección de datos de carácter personal, en el sexto apartado se analizará la Ley de Servicios de la Sociedad de Información y de Comercio Electrónico (LSSI) la cual se encarga del tratamiento de datos en el ámbito de Internet.

Para concluir esta guía, puede encontrar en los siguientes apartados las conclusiones obtenidas, la bibliografía, así como una serie de anexos para reforzar sus conocimientos adquiridos a lo largo de este documento.

SISTEMAS DE INFORMACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN:

Desde siempre, los recursos más importantes para cualquier empresa han sido el capital, la materia prima, el trabajo, los empleados entre otras cosas. Pero la sociedad ha ido avanzando y durante las tres últimas décadas se han incorporando numerosos avances dentro del ámbito de las organizaciones como pueden ser los ordenadores y las nuevas telecomunicaciones.
En la actualidad, la información es el recurso de mayor importancia de las empresas. La información es un recurso vital y el manejo de ésta puede conducir al éxito de los proyectos que se emprenden dentro de la empresa o por el contrario al fracaso si su manejo no es el debido. Para salir exitosos tendremos que hacer un manejo eficiente de la información y el conocimiento y combinarlo con una buena estrategia de negocios.

Y del mismo modo que se tiene gran cuidado por los recursos de la empresa, también la información requiere de cuidados y atención.

La forma de cuidar esta información es manejarla a través de un Sistema de Información, el cual nos permite comprender y analizar todos los datos generados por las actividades que nuestra organización lleva a cabo.
Con el manejo de la información, podemos lograr nuevas ventajas competitivas a través de su implantación y uso, obtener mayores niveles de capacidad de desarrollo y oportunidades de negocio.
Además, este manejo de información nos permite conocer las fortalezas y debilidades de nuestra organización de modo que podremos identificar las áreas de la empresa que necesitan de mayor atención por parte de los directivos y en definitiva, por parte de todos los integrantes de la organización.

Hasta ahora sabemos que la información se maneja con Sistemas de Información, ¿pero qué es un Sistema de Información?
Un Sistema de Información es un conjunto organizado de elementos que interaccionan entre si para lograr un objetivo común. Estos elementos pueden ser personas, datos, actividades o técnicas de trabajo y recursos materiales en general.
Esta interacción entre los distintos elementos se produce para poder procesar los datos y la información y poder distribuirla de la manera más adecuada posible entre la organización, siempre teniendo en cuenta los objetivos marcados.
Básicamente, el objetivo primordial de la información es el apoyo a la toma de decisiones de los gerentes ya que los Sistemas de Información no toman decisiones sino que son un mecanismo que ayudan a tomarlas. La elección de una decisión u otra queda en manos del directivo para lo cual necesitará adquirir una visión tanto global como empresarial de los Sistemas de Información.

Es impensable para una empresa, ya sea grande, mediana o pequeña, el querer crecer y no contar con un Sistema de Información, ya que esta es una herramienta que proporciona a las empresas grandes oportunidades.

Los Sistemas de Información cumplen unos objetivos básicos dentro de las organizaciones como son la automatización de los procesos, la ayuda en la toma de decisiones, que ya hemos comentado anteriormente, y el control que nos permiten ejercer sobre todos los elementos de la empresa y los recursos que la integran.

A menudo, solemos utilizar el término Sistemas de Información y el término Tecnología de los Sistemas de Información como sinónimos, pero esto es erróneo.

Las Tecnologías de los Sistemas de Información son un conjunto de servicios, redes, software y dispositivos que pueden formar parte de un Sistema de Información como recurso material, pero que nunca se podrá considerar como Sistema de Información en sí.
Estas tecnologías se encargan de básicamente del diseño, desarrollo, fomento, mantenimiento y administración de la información a través de los sistemas informáticos y comunicación ya que no solamente hablamos de los ordenadores, sino que también incluimos las redes de telecomunicaciones, la telemática, la telefonía, la televisión, la radio, los dispositivos portátiles y otros.

Las Tecnologías de los Sistemas de Información tomarán un papel u otro en una determinada organización dependiendo de las necesidades de negocios o del cumplimiento de los objetivos de ésta. Esto es debido, a que por sí solas no son verdaderamente útiles en términos empresariales, sino que son un medio de apoyo para conseguir los objetivos fijados de forma más eficaz y eficiente.

Como ya habíamos comentado anteriormente, los Sistemas de Información permiten obtener a las organizaciones una serie de ventajas competitivas. Para ello, será necesaria una adecuada coordinación de la planificación estratégica de la empresa con la planificación de los Sistemas de Información y esto nos llevará a tener unas necesidades de apoyo y soporte que podremos suplir con las Tecnologías de la Información.

Debido a que estos dos conceptos están en auge en estas últimas décadas, todas les empresas dedican gran parte de sus recursos a incorporar en ellas estos sistemas y tecnologías. Por ello la gran importancia de renovar e innovar en Sistemas y Tecnologías de Información si se quiere sobrevivir al mercado actual.

Sintetizando los conceptos anteriores, concluimos que tanto los Sistemas de Información como las Tecnologías de los Sistemas de Información influyen de forma directa o indirecta en los negocios de las organizaciones. Que además, estos Sistemas y Tecnologías en sí mismo no aseguran a la empresa el éxito, sino que son una ayuda para conseguirlo ya que el éxito en gran parte se debe a las decisiones de los gerentes y al trabajo de todo el personal de la empresa.

LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: LA LOPD

La principal normativa que se encuentra en vigor en España actualmente es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) la cual entró en vigor en España el pasado 14 de enero de 2000, derogando, en consecuencia, la Ley Orgánica 5/1992, de 29 de octubre, de regularización del tratamiento automatizado de los datos de carácter personal (LORTAD) que era la ley que estaba vigente en España hasta ese momento.

La LOPD es el resultado de la transposición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, y el objeto que pretende esta ley es garantizar las libertades públicas y los derechos fundamentales de las personas físicas en lo que concierne al tratamiento de los datos personales, especialmente de su honor, intimidad y privacidad personal y familiar. Además, esta Ley establece las obligaciones relativas a la recogida de datos, consentimiento, almacenaje, conservación, uso, datos especialmente protegidos, comunicación o cesión de los mismos y transferencias internacionales de los datos.

Esta Ley obliga a las empresas que operan con datos de carácter personal a protegerlos y a informar de la existencia de ficheros que los contienen. Además impone una serie de obligaciones legales para todas aquellas personas tanto físicas como jurídicas que posean ficheros con datos de carácter personal.

El ámbito de aplicación de esta nueva Ley se ha visto ampliado ya que ahora afecta a todos los ficheros de datos, estén informatizados o no, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, sea cual sea el soporte o medio de tratamiento. La LOPD resuelve el vacío legal existente desde la LORTAD, de los ficheros no automatizados.
Además, ésta también introduce otras modificaciones como la creación de la figura del encargado del tratamiento que junto con los responsables de los ficheros soportan una gran responsabilidad y pueden ser multados si realizan alguna infracción.

La LOPD ha tomado mucha importancia en los últimos años debido a que convierte el derecho a la protección de los datos personales en un derecho fundamental de las personas. Este derecho fundamental tiene su origen en la Constitución Española del 6 de diciembre de 1978 ya que en el artículo 18 de la Constitución se encuentra el derecho a la intimidad y al honor. El artículo 18.4 es el más representativo de lo ya comentado, "*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*". Destacar que este artículo no menciona explícitamente a los datos de carácter personal, pero se considera que éstos forman parte de la intimidad de las personas.

La LOPD se apoyó en el Reglamento de Medidas de Seguridad (RMS, Real Decreto 994/1999 de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal de 11 de junio de 1999). El RMS regulaba las medidas técnicas y organizativas que debían de aplicarse a los sistemas de información que trataran datos de carácter personal de forma automatizada.
El RMS fue derogado en 1999 por el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal (RDLOPD, aprobado en Consejo de Ministros

de 21/12/2007 y publicado en el Boletín Oficial del Estado el 10 de enero de 2008) y desarrolla de forma completa la LOPD. Este Reglamento es de obligado cumplimiento para todas aquellas empresas que posean ficheros de carácter personal, lo que hace que sea aplicable a la totalidad de las mismas.
El RDLOPD surgió debido a que la LOPD es una ley muy general, la cual pretende aplicarse a infinidad de supuestos diferentes. De tal forma que se desarrolló este Reglamento que desarrolla y concreta la Ley al máximo, de modo que se consigue una adaptación a la realidad actual a distintos sectores.
El Reglamento establece las normas, medidas, procedimientos y mecanismos que obligatoriamente se han de seguir para garantizar la seguridad y protección de los datos de carácter personal que están en ficheros tanto automatizados como no automatizados, afectando a sistemas informáticos, archivos de soportes de almacenamiento, procedimientos operativos, personal y otros.

El derecho fundamental a la protección de datos pasó a ser un derecho autónomo e independiente del derecho de intimidad como consecuencia de la Sentencia 292/2000 del Tribunal Constitucional de 30 de noviembre.

La LOPD consta de cuarenta y nueva artículos divididos en siete títulos y en una parte final compuesta por seis disposiciones adicionales, tres disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

Las obligaciones impuestas por la LOPD se pueden resumir en tres obligaciones básicas que son legalizar, legitimar y proteger.

En primer lugar se deberá inscribir y legalizar todos los ficheros de datos de carácter personal ante el Registro de la Agencia Española de Protección de Datos. Para ello es necesario que la empresa identifique los datos de carácter personal que se manejan y que indique en el registro también la forma de organizarlos que se lleva en la empresa.

Luego, hay que saber que todos los datos de carácter personal recogidos por la empresa deben contar con el consentimiento del afectado y cumplir con unos principios básicos: Principio del consentimiento del afectado, Principio de información y Principio de calidad de los datos. Todos estos principios serán expuestos más adelante.

Por último, la LOPD y el Reglamento de Medidas de Seguridad establecen la obligación de establecer una serie de medidas para garantizar la protección y seguridad de los datos. Estas medidas deben ser adoptadas por la empresa que almacena los datos. La medida de mayor importancia es la elaboración de un Documento de Seguridad en el que se detallarán los datos almacenados, las medidas de seguridad adoptadas y las personas que tienen acceso a esos datos. Una vez implantado en la empresa el Documento de Seguridad, se deben implantar los procedimientos y medidas de seguridad incluidas en dicho Documento de Seguridad y se debe realizar un seguimiento continuo de la implantación.

Pero el cumplimiento de la LOPD y su normativa de desarrollo no solo incumben estas tres obligaciones expuestas, sino que además se debe hacer un riguroso hincapié en su aplicación práctica en el seno de las organizaciones. El incumplimiento de la LOPD conlleva grandes responsabilidades a la organización y a todo su personal que trate o acceda a datos de carácter personal. Y ya no sólo hablamos de responsabilidades

administrativas, sino que ahora también incluimos responsabilidades civiles, penales y laborales.

Por este motivo, es imprescindible informar y formar al personal sobre la LOPD y se puede conseguir de diferentes formas como por ejemplo mediante el establecimiento de una Política de Tratamiento de Datos en la Organización o mediante la formación del personal en materia de protección de datos.

La adaptación a la normativa sobre protección de datos es una tarea que exige un seguimiento constante, por ello el esfuerzo de las empresas debe ser continuo.
Las empresas pueden contratar asesoramiento externo para la implantación de las medidas de protección de datos.
Podemos encontrar más información sobre la aplicación de medidas para la protección de datos en la página web de la Agencia Española de Protección de Datos (www.agpd.es), la cual dispone de un Canal de Responsables de Ficheros que ofrece información detallada sobre las implicaciones de la normativa sobre protección de datos para las empresas así como pautas para su correcta implementación.
También en la web del Instituto Nacional de Tecnologías de la Comunicación (www.inteco.es), donde hay disponible un catálogo de consultores de negocio. Este catálogo incluye una lista de profesionales especializados en seguridad y protección de datos.
Y además, se puede hacer uso de paquetes software que pretenden ser un apoyo tanto en la implantación de la normativa como en el mantenimiento posterior.

Hay una serie de motivos con los que se demuestra la gran importancia de proteger los datos personales y los que justifican en gran medida la creación de la LOPD.

Uno de estos motivos es que los datos personales son un activo valioso para las empresas cuyo valor reside en el hecho de ser indispensable, en muchos casos, para continuar con la actividad de la empresa. Hay que realizar un esfuerzo en proteger estos datos para garantizar su confidencialidad y evitar posibles incidencias de seguridad como la pérdida, fuga o robo de información.

Otro motivo es el hecho de que la adaptación a la LOPD contribuye a aumentar la calidad de las operaciones de la empresa y a mejorar los procesos de manejo de la información. También decir que las empresas que garantizan la protección de los datos personales que manejan ofrecen mayor confianza y su imagen corporativa mejora.

Pero el motivo más importante y del cual ya hemos hablado es que la protección de datos es un derecho fundamental y por tanto se debe velar por su garantía y respeto.
La Agencia Española de Protección de Datos puede realizar inspecciones a las empresas y sancionar a las que incumplen la normativa.

ANTECEDENTES A LA LOPD: LORTAD

La Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD) fue la ley predecesora a la actual LOPD.

Esta Ley fue impulsada por el mandato constitucional contenido en el artículo 18 punto 4 de la Constitución Española, pero además hay otros tres documentos europeos claves que influyeron en la creación de esta Ley:

-El Convenio de Europa, de 28 de enero de 1981, para la protección de las personas con relación al tratamiento automatizado de datos de carácter personal, ratificado por España el 27 de enero de 1984. Este convenio proponía un equilibrio entre el respeto a la vida privada y la libre circulación de la información entre pueblos.

- El Acuerdo de Schengen, de 14 de junio de 1985, que tiene como objetivo la supresión de los controles entre las fronteras comunes de los países firmantes del acuerdo y la libre circulación de personas entre los países.

-La Propuesta de Directiva del Consejo de la Comunidad Económica Europea, de 24 de septiembre de 1990, relativa a la protección de las personas en lo referentes al tratamiento de datos personales. Hoy en día se trata de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

En marzo de 1993 se creó la Agencia Española de Protección de Datos, el cual era un organismo independiente que debía garantizar el cumplimiento de los mandatos que se establecían en la LORTAD.
La Agencia actúa como inspectora, ordenadora, reguladora, sancionadora, unificadora, inmovilizadota y relaciones públicas.

La LORTAD sólo estuvo vigente siete años en el régimen jurídico español. Desde el 15 de enero de 2000, la ley vigente en materia de protección de datos es la LOPD.
La LOPD mantiene vigentes algunos aspectos de la LORTAD y modifica o inserta otros aspectos. En este sentido se establece que se mantiene la vigencia de la LORTAD *"en todo lo que no se oponga a la Ley".*

La diferencia fundamental entre ambas es el ámbito de aplicación, ya que la LORTAD solamente abarcaba los ficheros de datos personales que se almacenaban en soporte electrónico, es decir, automatizados, y en cambio, en la LOPD el ámbito de aplicación se amplía y a abarca los ficheros de datos de carácter personal automatizado y los no automatizados.

CUESTIONARIO DE ADECUACIÓN A LA LOPD

Para saber si su empresa está adecuada a la LOPD, le proponemos un simple cuestionario que debe contestar. Si alguna de las contestaciones resulta ser un "no", significa que su empresa no cumple la legislación vigente en temas de protección de datos de carácter personal. En este caso usted deberá seguir con exactitud esta Guía de cumplimiento que le ayudará a entender todos los artículos de la Ley y a saber actuar en cada momento.
Esta serie de preguntas las podemos encontrar en varias páginas webs de empresas que se dedican a la consultoría.

1. ¿Dispone de ficheros en sus sistemas informáticos que incluyan datos personales relativos a personas físicas?

2. ¿Ha inscrito dichos ficheros, con carácter previo a su creación, en la Agencia de Protección de Datos?

3. ¿Cumple con el deber de información en la recogida de datos que establece la LOPD?

4. ¿Solicita el consentimiento de los titulares para llevar a cabo el tratamiento de datos de carácter personal?

5. ¿Cuándo recaba datos de una persona distinta del interesado, se le informa de ello?

6. Los datos de que dispone ¿son exacto y los mantiene actualizados?

7. ¿Ha determinado por medio de contrato escrito el acceso a los datos que pueda tener cualquier empresa que le preste un servicio?

8. ¿al ceder los datos por primera vez, informa a los afectados indicando la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y la dirección del cesionario?

9. ¿Dispone de un documento de seguridad donde se establezcan las medidas de seguridad aplicables a su empresa o negocio?

10. ¿Ha establecido algún procedimiento para que los interesados ejerciten sus derechos de oposición, acceso, rectificación o cancelación de los datos?

Pero ahora, desde la propia página web de la Agencia Española de Protección de Datos, una empresa puede obtener un diagnóstico sobre su situación ante la LOPD, simplemente contestando a una serie de preguntas con respuestas múltiples de forma on-line. Esta herramienta se llama "Evalúa".
Una vez realizado el autotest, que lleva de 45 a 60 minutos, la AEPD facilitará un informe con indicaciones y recursos que puedan orientar a la empresa para poder cumplir con lo dispuesto en la LOPD.
Hay que tener en cuenta que este test es completamente anónimo y que el test es meramente orientativo.

ANÁLISIS DE LA LOPD

- **OBJETO**

El objeto de la LOPD es el de "*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*" tal como se expone en el artículo 1 de esta ley.
Todas las empresas y organismos públicos tratan con datos de carácter personal y por este motivo están obligados a garantizar el derecho a la protección de datos personales para que no sean utilizados de forma inadecuada, ni tratados o cedidos a terceros sin consentimiento del titular.
Este derecho fundamental nace a partir de los artículos 10 y 18.4 de la Constitución Española.

"10.1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la Ley y a los derechos de los demás son fundamento del orden político y de la paz social.
10.2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los Tratados y acuerdos internacionales sobre las mismas materias ratificados por España."

"18.4. 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."

- **ÁMBITO DE APLICACIÓN**

El ámbito de aplicación de la LOPD se expone en el artículo 2 y está estructurado en tres puntos básicos: casos en que la Ley Orgánica sí es de aplicación, casos en que la Ley Orgánica no es de aplicación y casos en que el tratamiento de protección de datos se regirá por disposiciones especiales.

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*".
Apreciamos con claridad que todos los datos que estén en soporte informático o telemático son del ámbito de aplicación ya que son ficheros automatizados los cuales para su creación se exige la grabación, depuración y estructuración de una forma determinada. En cambio, los ficheros en soporte de papel o ficheros no automatizados nos plantean dudas a la hora de incluirlos en el ámbito de aplicación de la ley.
Según la Agencia Española de Protección de Datos, la documentación en papel forma parte de un fichero no automatizado siempre que "*el conjunto de datos se encuentre estructurado con arreglo a criterios referidos a personas físicas*". Por otra parte, "*puede que el fichero no esté directamente estructurado con arreglo a este criterio, pero los criterios de organización permitan detectar sin esfuerzos*

excesivos la información referida a una persona física". En este caso sí se aplican la LOPD y el RDLOPD.
Recalcar que las empresas están acostumbradas a controlar el acceso a los ficheros informáticos, pero esta medida de seguridad no se aplica en cambio a los documentos en soporte en papel. Al hablar de documentos en soporte papel, el control de acceso debe ser físico y ello dificulta tanto la aplicación como la continuidad de esta medida. Sólo el 37% de las empresas españolas disponen de normas de seguridad específicas para proteger los datos de carácter personal en soporte papel. (PricewaterhouseCoopers 2006)

Hay que tener muy en cuenta que el fichero de personal de la empresa, debido al alcance de sus datos y a su finalidad, estará siempre sometido a la LOPD.

Pero dentro de estos casos donde sí es de aplicación la LOPD, aparecen en el artículo 2 del Reglamento varias excepciones.
Si los datos de los ficheros se limitan, en el caso de personas de contacto (artículo 2.2), *"a los nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales"* y en el caso de comerciantes (artículo 2.3) a datos vinculados exclusivamente con la actividad empresarial y además el destinatario del tratamiento de los datos es una empresa y nunca una persona física, entonces los ficheros están exentos de la aplicación de la LOPD y del RDLOPD.
Hay que recalcar que el DNI no es un dato enumerado por el artículo 2.2, de modo que si se tiene el DNI de las personas de contacto, entonces no opera la excepción.

Quedan excluidos de la aplicación de la LOPD los ficheros mantenidos por personas físicas que se utilizan exclusivamente en el ámbito personal o doméstico, los ficheros que se rigen por la normativa de materias clasificadas y los ficheros establecidos para temas de terrorismo o delincuencia organizada.

En cuanto a los casos en que el tratamiento de datos se rige por disposiciones especiales nombramos a modo de ejemplo alguno de ellos, porque usted como empresario de una empresa privada pequeña no contará con este tipo de ficheros. Alguno de ellos son los ficheros regulados por la legislación de régimen electoral o los derivados del Registro Civil y del Registro Central de penados y rebeldes.

El ámbito de aplicación del Reglamento será diferente en función de si los ficheros de su empresa han sido notificados al Registro General de Protección de Datos antes o después de su puesto en vigor.
Si usted inscribió los ficheros antes se aplicarán en general las disposiciones del Reglamento desde la fecha de su entrada en vigor, salvo las excepciones derivadas de las disposiciones transitorias del Real decreto 1720/2007 en materia de seguridad.
En cambio, a todos los ficheros que no han sido inscritos en el Registro antes de la entrada en vigor del Reglamento, se les aplicará la totalidad de las disposiciones desde el momento de su entrada en vigor.

- **CALIDAD DE LOS DATOS**

Los datos que obtenga para crear los ficheros deben de seguir una serie de principios generales de Calidad. Principios que se desarrollan en el artículo 4 de la LOPD.

En primer lugar, la LOPD establece que los datos personales deben ser recogidos exclusivamente para la finalidad para la que fueron recabados y no para otros diferentes.
Si por determinadas razones la finalidad de alguno de sus ficheros cambia, entonces los datos deberán ser cancelados y deberá crear un nuevo fichero y establecer la nueva finalidad.
Es muy importante cuando recoja datos personales determinar, en las cláusulas de información, todas las finalidades a las que se van a destinar los datos.
Por otra parte, sí que se permite el tratamiento de los datos con fines distintos a los iniciales en el caso de uso posterior para fines históricos, estadísticos o científicos. Además, según la Guía del Responsable de Ficheros, documento elaborado por la AEPD, también está permitido *"conservar datos que ya no sean necesarios de acuerdo al tratamiento para el que hubieran sido recogidos"* en los casos de valor histórico, estadístico o científico fijado por Ley.

Otro principio que sus datos deben seguir es el hecho de que éstos deben ser exactos y actualizados ya que deben responder *"con veracidad a la situación actual del afectado"*.
Existe una presunción de que los datos facilitados en un determinado momento por un cliente son exactos pero en caso de que su empresa fuera sabedora de la inexactitud se debe actualizar o cancelar de inmediato.
La inexactitud de un dato puede conocerse por ejemplo a causa del ejercicio por parte del afectado de sus derechos o por la comunicación de una resolución judicial o administrativa en que se manifieste el error.
La corrección o actualización de los datos puede ser realizada por el Responsable del Fichero o por el propio interesado por medio del ejercicio del derecho de rectificación de datos.
Como ya hemos comentado con anterioridad, existen unas fuentes de datos accesibles al público como son los repertorios telefónicos o los boletines oficiales. En estos casos, el Responsable de Fichero de su empresa no es el responsable de comprobar la exactitud de los datos obtenidos de estas fuentes, pero de todos modos, si es conocedor de alguna inexactitud en algún dato debe rectificarlo.

Una vez terminada la finalidad de tratamiento de los datos que se recogieron, el Responsable del Fichero debe cancelarlos. Sólo deben ser conservados el tiempo necesario para las finalidades establecidas.
Como excepción a este principio, sólo una obligación legal puede permitirle la conservación de datos cuya finalidad que motivó su recogida esté ya concluida. En este caso, el Responsable del Fichero conservará los datos a través de dos métodos que estudiaremos más adelante: el bloqueo del dato y el proceso de disociación.

En cuanto al almacenamiento de los datos, éstos deben permitir el ejercicio de los derechos de acceso por parte del afectado, salvo que sean legalmente cancelados.

Por último, dentro de los principios de Calidad de los Datos, se debe asegurar que todos los datos recogidos han sido obtenidos de forma lícita. Se prohíbe totalmente recoger datos de forma fraudulenta, desleal o ilícita.

El incumplimiento de cualquiera de los principios de Calidad de los Datos se considerará como una infracción grave o muy grave (artículo 44 de la LOPD).
De este modo las vulneraciones graves de los principios de Calidad se consideran infracción grave:

-*"Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad"* (Art.44.3.b)

-*"Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidas en la Ley o con incumplimiento de los preceptos que impongan las disposiciones reglamentarias de desarrollo, cuando no constituyan infracción muy grave"* (Art.44.3.d)

-*"El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada"* (Art.44.3.e)

-*"Mantener los 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"* (Art.44.3.f)

Y se considera infracción muy grave:
-*"La recogida de datos de forma engañosa y fraudulenta"* (Art.44.4.a)

- **<u>DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS</u>**

Cuando usted vaya a obtener datos de carácter personal de algún interesado debe informarle de *"modo expreso, preciso e inequívoco"* sobre la existencia de los ficheros en los que serán incluidos sus datos, para qué se van a utilizar esos datos, de los destinatarios de esta información; de la identidad, dirección y forma de contacto con el Responsable y Encargado de Tratamiento de los ficheros; de la posibilidad que tiene de conocer los accesos que se produzcan a sus datos y la de ejercer los derechos de acceso, rectificación, cancelación y oposición. Además, se informará sobre el *"carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas"* al titular (artículo 5.1.b LOPD) y de las consecuencias de la obtención de los datos o de la negativa de suministrarlos.

En el caso en que algún dato dado por el interesado se pueda deducir de la naturaleza de los propios datos personales o de las circunstancias en que se recogen, entonces no se estará usted obligado a informar al titular sobre la inscripción de ese dato en los ficheros de la empresa. Un ejemplo sencillo es la edad del interesado, ya que si ha recogido su fecha de nacimiento, su edad se deduce fácilmente.

Si el Responsable del tratamiento no está establecido en el territorio de la Unión Europea pero utiliza en el tratamiento de datos medios que sí están situados en territorio español, entonces, éste deberá designar un representante en España.

Toda la información comentada en el primer párrafo debe estar incluida en los cuestionarios o documentos de recogida de datos que debe preparar para obtener estos datos.
Hay diversas formas de informar a los titulares sobre la recogida de sus datos.
En el caso en que los datos sean recogidos directamente, a los interesados se les tendrá que informar antes de la obtención de éstos.
Si el interesado debe rellenar un formulario con sus datos para que el Responsable del tratamiento haga uso de ellos, debe aparecer al final de dicho documento información acerca de esta recogida y sobre el derecho de acceso a estos datos por parte del interesado. De modo que deberá aparecer un texto similar al siguiente:

"Los datos personales recogidos mediante este formulario serán tratados de forma confidencial y serán registrados, en su caso, en el fichero automatizado (nombre del fichero) titularidad de (nombre del Responsable del fichero), con la finalidad de (finalidad de este fichero). Ud. podrá ejercer los derechos de acceso, cancelación, rectificación y oposición mediante escrito dirigido a: (dirección y forma de contacto con el Responsable y Encargado del fichero)."

Puede, en otras circunstancias que se utilice un cartel informativo el cual debe contener todas las exigencias del artículo 5 de la LOPD o al menos complementarse con la existencia de hojas informativas a disposición de los usuarios. Por ejemplo, si usted instala cámaras de vigilancia en su empresa puede informar a los usuarios sobre sus derechos respecto a este hecho, mediante un cartel informativo que indique: *Instrucción 1/2006 de la AEPD – videovigilancia.* Así que los usuarios deben de dirigirse a esta instrucción para ser conocedores de sus derechos.
Este ejemplo se ha obtenido de un documento de FAQs de la AEPD realizado a raíz de la 1ª sesión anual abierta de la AEPD el 22 de abril de 2008.

Si por el contrario, los datos son recogidos mediante una aplicación informática a través de Internet, se deberá también informar antes de empezar la recogida de datos. Lo más utilizado en las páginas webs son las políticas de privacidad, los avisos legales o cláusulas de protección que acceden a través de enlaces a documentos que invitan a conocer todas las exigencias del artículo 5 de la LOPD comentadas anteriormente y que sin su aceptación, marcando una casilla similar a: "He leído y acepto estas condiciones", no se puede avanzar en el proceso de obtención de datos, de modo que siempre la información ha de ser previa a la obtención. Estos procedimientos a través de las aplicaciones web tienen como fin el asegurar que el consentimiento de los afectados sea efectivamente específico e inequívoco.

Una aplicación online, *glosario.net,* define a política de privacidad como el documento que especifica los procedimientos, reglas y prácticas de seguridad de datos que realiza una empresa con las que garantiza el mantenimiento de la integridad, confidencialidad y disponibilidad de la información que recode de sus cliente y de otros interesados titulares de datos, de conformidad con la legislación

vigente, las necesidades de seguridad informática y objetivos de negocio que persiga.

Es necesario poder acreditar el cumplimiento del deber de información cuando los datos se recogen a través de un formulario web, por ejemplo la constancia de la fecha en el acceso a la página web.

También existe la posibilidad que usted obtenga datos de titulares los cuales no se los haya facilitado el mismo titular y por este motivo el Responsable del Fichero de su empresa o su representante debe informarle de este hecho dentro de los tres meses siguientes del registro de dichos datos.
La AEPD califica este derecho de información en la recogida de datos como un derecho esencial ya que garantiza que el consentimiento que se preste sea previo.

- **CONSENTIMIENTO PARA EL TRATAMIENTO DE LOS DATOS**

El artículo 3.h de la Ley Orgánica 15/1999 define el consentimiento como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen"*, salvo que la ley disponga otra cosa.

Estos cuatro requisitos enumerados son indispensables y por ello vamos a hondar más en su significado.

El consentimiento debe ser obtenido libre de vicio alguno y debe ser específico para cada tratamiento y para cada finalidad, explícita y legítima del Responsable del Fichero.
El requisito de información es el que ya hemos estado estudiando, el cual establece que los usuarios deben saber, antes de la recogida de sus datos, la existencia y la finalidad de los ficheros.
E inequívoco se refiere a que es necesario que exista una acción u omisión que implique la existencia del consentimiento.

Una vez el afectado es informado en el proceso de obtención de sus datos de las exigencias del artículo 5 de la LOPD, se entiende que el afectado es consciente de todas ellas y que las acepta y da su consentimiento y aprobación.

Pero habrá casos en los que no será necesario el consentimiento previo del afectado para el tratamiento de sus datos personales, como por ejemplo en caso de tratamientos realizados por Administraciones Públicas; tratamientos que se realizan para mantener una relación precontractual, contractual, laboral o administrativa; tratamientos necesarios para proteger un interés vital del interesado o de otra persona; cuando se trate de datos procedentes de fuentes públicas y otros.

En término generales, sin el consentimiento del afectado, no se considerará lícito la posesión de sus datos y además legalmente puede ocasionar una infracción grave de acuerdo con el artículo 44.3.c de la LOPD: *"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"*, o una infracción muy grave de acuerdo con el

artículo 44.4.c: *"Recabar y tratar los datos de carácter personal a los que se refiere el artículo 7.2 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos a los que se refiere el artículo 7.3 cuando no lo disponga una ley o el afectado no haya consentido expresamente".*

- **Consentimiento para el tratamiento de datos de menores de edad**

Los mayores de 14 años podrán dar su consentimiento para el tratamiento de sus datos excepto aquellos mayores de 14 años que por Ley se exija la asistencia de los titulares de la patria potestad o tutela.

En el caso de los menores de 14 años, también será necesaria la presencia de los titulares de la patria potestad o tutela.

Si usted obtiene datos de menores, debe saber que no se permite obtener información que pueda hacer referencia a familiares sin el previo consentimiento de éstos. Pero tal y como indica en el artículo 13 del RDLOPD sí *"podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización (...)"* para proceder al tratamiento del menor.

Al dirigirse a los menores para obtener su consentimiento, hay que utilizar un lenguaje fácil de entender por ellos.

- **<u>REVOCACIÓN PARA EL TRATAMIENTO DE LOS DATOS</u>**

El afectado puede revocar en cualquier momento el consentimiento que hubiera prestado al recogerse sus datos, siempre y cuando exista una causa justificada, aunque realmente la causa justificada se exige en aquellos casos en los que el tratamiento de los datos procede del mantenimiento de una relación de negocios, administrativa, laboral o fiscal.
No se exigirá una causa justificada para la revocación del consentimiento en los casos de cesión de datos o cuando el fin de los datos sea promocional o publicitario.

Existen algunos casos en que no es necesario el consentimiento del afectado para el tratamiento de los datos personales, así que en estos supuestos, el afectado podrá oponerse a su tratamiento siempre y cuando existan *"motivos fundados y legítimos relativos a una concreta situación personal"* (artículo 6.4 LOPD). El Responsable del Fichero de su empresa deberá entonces excluir el tratamiento los datos de la persona que se oponga.

Se establece un plazo 30 días para que los afectados se opongan al tratamiento de sus datos, y se les deberá advertir que en caso de no pronunciarse se entenderá que sí consienten el tratamiento.
Los afectados deben disponer de un medio fácil y gratuito para oponerse al tratamiento de sus datos. Por ejemplo, pueden enviar un prefranqueado al Responsable del Tratamiento de su empresa, pueden llamar a un número telefónico gratuito o a los servicios de atención al público (artículo 14 del RDLOPD).

Un vez el Responsable del Fichero recibe la revocación del afectado, hay un plazo máximo de 10 días para que el Responsable deje de tratar con estos datos.
Si los hubiera cesado a otros antes de la revocación, el propio Responsable debe comunicarlo a los cesionarios.

- **DATOS ESPECIALMENTE PROTEGIDOS Y DATOS RELATIVOS A LA SALUD**

Hay una serie de datos que son considerados como datos especialmente protegidos y por tanto el afectado tiene derecho a no dar su consentimiento para su tratamiento.
A esto datos se le otorga un mayor grado de protección y se impone una serie de obligaciones especiales a los Responsables de Fichero para obtener el consentimiento de los afectados.

Los datos especialmente protegidos corresponden al ámbito de la intimidad personal y familiar de los afectados y no al ámbito profesional. Se consideran datos especialmente protegidos los que revelan información acerca de la ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual y comisión de infracciones o administrativas.
La Constitución Española establece en el artículo 16.2 que *"Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias"*

El apartado 45 de la Memoria Explicativa del convenio 108 del Consejo de Europa define los datos de carácter personal relacionados con la salud como las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo, incluyendo los referidos a los porcentajes de discapacidad y su información genética, así como las informaciones relativas al abuso del alcohol o al consumo de las drogas".

El Responsable del Fichero de la empresa es el encargado de informar sobre este derecho al afectado cuando se vayan a obtener datos de carácter personal.

Es necesario un consentimiento expreso y por escrito por parte del afectado para que el Responsable del Fichero pueda tratar los datos que revelen la ideología, afiliación sindical, religión y creencias de éstos.
Las entidades sin ánimo de lucro cuyo fin sea político, religioso, filosófico o sindical están exentas.

En cambio, los datos de carácter personal referentes al origen racial, salud o vida sexual y los datos relativos a la salud podrán ser recabados, tratados o cedidos si hay un consentimiento expreso por parte del afectado, si lo dispone una ley o si son necesarios para el diagnóstico o tratamiento médico.

Del mismo modo, la propia Ley prohíbe totalmente crear ficheros con la única finalidad de almacenar información sobre ideologías, afiliaciones sindicales, religión, creencias, origen racial o vida sexual.

Al igual que en al apartado *"Consentimiento para el tratamiento de los datos",* usted podría cometer una infracción grave o muy grave de acuerdo a los artículos

44.3.c y 44.4.g de la LOPD si no cumpliera con las indicaciones de esta Guía de cumplimiento.

- **SEGURIDAD EN LOS DATOS**

El Responsable de los ficheros y el Encargado de los tratamientos deben garantizar la seguridad de los datos obtenidos por los afectados. Para ello deben desarrollar medidas y métodos de seguridad y crear un Reglamento de medidas de seguridad en el cual profundizaremos en apartados siguientes.

- **DEBER DE SECRETO**

Todas las personas de su empresa que participan o que hayan participado en el tratamiento de datos de carácter personal de otros, tiene la obligación de guardar secreto. De modo que no podrán comunicar a terceras personas la información a la cual son accesibles por el cargo que desempeñan.
También en el artículo 5.a del Estatuto de los Trabajadores se refleja esta obligación profesional de confidencialidad y de secreto*:"Deberes laborales. Los trabajadores tienen como deberes básicos: a) Cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad a las reglas de la buena fe y diligencia."*

El cumplimiento de unas medidas de comportamiento por parte del personal de la empresa, y en especial de aquel personal que accede a los ficheros de datos de carácter personal, puede ayudar a garantizar la confidencialidad de la información dentro de la empresa.
En una guía práctica de adaptación a la LOPD consultada online nos proponen tres medidas básicas para el personal de la empresa:

-Deber de actuar siempre conforme a sus obligaciones profesionales de confidencialidad y secreto, así como de acuerdo a lo dispuesto por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y su normativa de desarrollo.

-Acceso a los datos personales únicamente por el personal autorizado, limitado a las funciones y actividades a desempeñar.

-No revelar información a personas ajenas que no deban tener acceso a dicha información.

El incumplimiento de este artículo 10 de la LOPD puede incurrir en infracciones de carácter grave - "*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"*(artículo 44.3.g) - o infracciones muy graves - *"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"(artículo 44.4.g).

- **COMUNICACIÓN O CESIÓN DE LOS DATOS**

Los datos de carácter personal objeto del tratamiento pueden ser cedidos a un tercero siempre que sea para *"fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"* (artículo 11).
Cuando se recabe el consentimiento del interesado, se le debe informar de la identidad, de la actividad y de la dirección del cesionario, así como de la finalidad a la cual se destinarán los datos cedidos. Si el interesado no es informado de alguno de estos aspectos entonces se considerará nulo el consentimiento.
Por otra parte, esta información no será necesaria comunicarla en el caso de que resulte imposible o exija grandes esfuerzos por parte de la Agencia Española de Protección de Datos.

Como excepción, hay una serie de casos en los cuales no es necesario el consentimiento del interesado como cuando la cesión está autorizada por Ley; cuando se trata de datos cedidos a entes públicos de la Administración o de ámbito jurídico; cuando se ceden datos relativos a la salud en situaciones de emergencia médica; cuando se trate de datos recogidos de fuentes accesibles al público; cuando sea necesario para el pleno cumplimiento de la relación contractual.

Por ejemplo, usted cede a una entidad financiera los datos de sus trabajadores para poder pagarles la nómina. Este caso es una de las excepciones enumeradas en el párrafo anterior ya que esta cesión no precisa del consentimiento de ninguno de sus trabajadores, dado que es necesario para el cumplimiento de la relación jurídica que vincula a usted como pagador a través de una entidad financiera y al destinatario, es decir sus empleados, y se justifica la cesión.

El consentimiento dado siempre es revocable, pero como bien indica la AEPD, esta revocación no tendrá efectos retroactivos a las cesiones que se realizaron mientras el consentimiento estaba activo.

Todo aquel al cual se le comunica o cede datos de carácter personal, debe al igual que usted como cedente y propietario originario de los datos, cumplir con todas las obligaciones y derechos dispuestos en la LOPD.

- **ACCESO A LOS DATOS POR CUENTA DE TERCEROS**

En primer lugar vamos a definir que es un *tercero* según la AEPD.
Tercero es cualquier persona física o jurídica, pública o privada u órgano administrativo distinto del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

El acceso a los datos por cuenta de terceros supone la prestación de un servicio al Responsable del fichero por parte de un tercero, que denominamos Encargado del tratamiento, el cual accede a los datos de un determinado fichero para el cumplimiento de la prestación contratada. El Encargado del tratamiento actúa en nombre, por cuenta y de acuerdo a las instrucciones establecidas y dadas por el Responsable del fichero.

La cesión de datos a un tercero no se considerará comunicación o cesión de datos tal y como hemos estudiado en el apartado anterior.

En este supuesto, este acceso deberá estar regulado por un contrato escrito o por otra forma que pueda acreditar su celebración y su contenido indicando las obligaciones del tratamiento. El artículo 12 de la LOPD regula el acceso a los datos por cuenta de terceros.

El tratamiento de los datos se regirá por las siguientes obligaciones:

- Sólo podrán ser tratados según las consideraciones del Responsable del Fichero. El Responsable fijará las instrucciones para el acceso y tratamiento.
- No podrán ser utilizados con un fin distinto al establecido en el contrato
- No se podrán comunicar a otras personas, aunque sean para su conservación.
- Se destruirán o se devolverán al responsable del tratamiento una vez cumplida la prestación contractual

Además, dicho contrato deberá incluir las medidas de seguridad elaboradas en su empresa y las cuales deberán ser implantadas para garantizar la seguridad de la totalidad de los datos y evitar pérdidas y tratamiento o accesos no autorizados.

Muchas veces, su empresa necesitará contratar o subcontratar la prestación de servicios con otras empresas. Estos servicios suponen un acceso por parte de un tercero a los datos de carácter personal que su empresa almacena.
En el caso de que fuera necesaria una subcontratación de los servicios, se podrá llevar a cabo siempre y cuando se cumplan los requisitos establecidos en el artículo 21.2 del RDLOPD:

- Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar
- Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del Responsable del fichero
- Que el Encargado del tratamiento y la empresa subcontratista formalicen el contrato previsto por el artículo 12 de la LOPD

Hasta este momento hemos analizado el supuesto en que el Responsable del fichero cede datos de su empresa a un tercero, llamado Encargado del tratamiento, perteneciente a otra empresa, para llevar a cabo una prestación de servicio.

Pero también cabe la posibilidad de que el Encargado del tratamiento tenga que subcontratar algún servicio que implique el acceso a los datos por parte de otro tercero. En este caso el Responsable del fichero deberá dar su consentimiento al Encargado del tratamiento por medio de un contrato.
Hay dos alternativas a la hora de realizar esta cesión de datos, bien se puede formalizar a través de un contrato a tres bandas, o se puede formalizar con la inclusión de una cláusula contractual en el contrato inicial. Esta cláusula expresará el consentimiento por parte del Responsable del fichero hacia el Encargado del tratamiento, para la subcontratación de servicios y/o actuaciones concretas que impliquen un acceso a los datos por parte de dicho tercero.

Si el Encargado del tratamiento al cual hemos comunicado los datos destina estos datos a una finalidad diferente a la establecida, los comunique o incumpla alguna de las exigencias del contrato, entonces deberá responder personalmente de las infracciones y sanciones interpuestas.

En el caso del Responsable del fichero, éste asumirá personalmente las infracciones cometidas por el Encargado del tratamiento siempre y cuando éste último haya actuado según las exigencias del contrato.

- **DERECHOS DE LAS PERSONAS**

Toda persona que sea titular de datos de carácter personal que estén incluidos en un fichero de tratamiento, tiene derecho, de forma gratuita, a solicitar al Responsable de un fichero o tratamiento, y a obtener de éste, información sobre esos datos, sobre el origen de esos datos, y sobre las comunicaciones que se han o van a realizar, Además también tiene derecho a actualizar esos datos si resultan ser inexactos o incompletos, a borrar datos también en el caso de que sean inexactos o si se han tratado de una forma ilegal y a oponerse a que se traten sus datos.
Estos derechos se podrán ejercer tanto en ficheros automatizados como en los no automatizados.

Estos derechos descritos en el párrafo anterior son los derechos básicos de las personas titulares de datos personales y son denominados derechos ARCO: derecho de acceso, derecho de rectificación y cancelación, y derecho de oposición.
Más adelante profundizaremos en ellos.

Los derechos ARCO son un pilar fundamental en la protección del honor, de la intimidad personal y familiar de los ciudadanos tal y como se dispone en el artículo 18.4 de la Constitución Española.
Garantizan a las personas el poder de control sobre sus datos personales.

- **Ejercitación de los derechos**

Los derechos ARCO son personalísimos que significa que solo pueden ser ejercidos por el titular de los datos acreditando su identidad, por su representante legal en el caso de que el afectado sea menor de edad o esté incapacitado, o a través de un representante voluntario que se debe designar expresamente para el ejercicio del derecho.

Del mismo modo, el Responsable del fichero deberá denegar el ejercicio de estos derechos si el solicitante no es el titular de los datos y no aporte la acreditación necesaria para representarlo.

Además, dichos derechos son independientes, es decir, que no se requiere para el ejercicio de ninguno de estos derechos, que previamente se haya ejercido otro.

Para el pleno ejercicio de los derechos, el Responsable del fichero deberá proporcionar al interesado un medio sencillo y gratuito. Hay que remarcar que el coste para los afectados a la hora de ejercitar sus derechos ARCO debe ser nulo. Por ejemplo, no sería válido como medio de ejercicio el envío de cartas certificadas o la utilización de servicios de telecomunicaciones de pago por parte del afectado.

Para el pleno ejercicio de estos derechos, los Responsables de los ficheros están obligados a facilitar este ejercicio y a dar una respuesta a los afectados dentro de los plazos establecidos por ley, con independencia del procedimiento utilizado por el interesado y de que se disponga o no de sus datos personales.

- **Procedimiento de ejercer los derechos**

Para proceder al ejercicio de los derechos, el interesado debe dirigir su comunicación al Responsable del fichero y le debe de adjuntar una serie de documentos: una fotocopia de un documento válido que lo identifique como puede ser el documento nacional de identidad o el pasaporte, o en el caso de representar a otra persona, los documentos acreditativos del representante; una petición en que se concreta la solicitud; la dirección a efectos de notificaciones, fecha y firma del solicitante; y el documento acreditativos de la petición que el afectado formula.

Aclarar que la AEPD no es la encargada de atender las solicitudes para el ejercicio de los derechos de los titulares, sino que esa labor es de los Responsables de los ficheros o tratamiento, de modo que en la AEPD nos pueden facilitar la dirección de este Responsable para poder ejercer los derechos de acceso, rectificación, cancelación u oposición.

Como ya se ha dicho, el Responsable del fichero debe contestar todas las solicitudes aunque en sus ficheros no figuren datos personales del solicitante.

- **Derecho de consulta al Registro General de Protección de Datos (RGPD)**

Cualquier persona podrá acceder al RGPD, el cual es de consulta pública y gratuita, y obtener información acerca de la existencia de tratamientos de datos de carácter personal, las finalidades de dichos tratamientos y la identidad del responsable de los tratamientos

Pero mediante la consulta al Registro no se puede conocer que empresas tienen en su poder datos personales nuestros, sino que sólo podemos conocer la información que los responsables de ficheros están obligados a notificar en el Registro: los datos del responsable del fichero, los datos para ejercicio de los derechos ARCO, la identificación y finalidad del ficheros, el origen y la procedencia de los datos, los

tipos de datos, la estructura y organización del fichero, la cesión y comunicación de datos y las transferencias internacionales.

Una persona puede acceder al Registro General de Protección de Datos a través de la página web de la AEPD, www.agpd.es, o dirigiendo un escrito al RGPD o al Director comunicándole los datos del afectado, el domicilio a efectos de notificaciones y el CIF de la empresa en cuestión, o personándose en las oficinas de la AEPD aportando el CIF de la empresa.

- **Derecho de impugnación de valores**

Este derecho nace con la finalidad de proteger la privacidad de los ciudadanos frente a la posibilidad de que se utilicen sus datos personales para evaluar determinados aspectos de su personalidad como pueden ser el rendimiento laboral o los hábitos, y se utilice la información obtenida para tomar decisiones que puedan afectar al ciudadano. Por ello, los afectados podrán impugnar estos actos administrativos o decisiones privadas.

Legalmente, no es obligatorio que los Responsable de los ficheros o tratamientos informen a los afectados de este derecho.

- **Derecho de acceso**

Mediante el derecho de acceso cualquier persona puede dirigirse al Responsable o Encargado de un fichero o tratamiento para recabar toda la información de sus datos personales que en la empresa en cuestión tenga en su poder.

Toda persona puede informase de los fines a los cuales sus datos están sometidos, del carácter del tipo de los datos, de su origen, de su destinatarios, y así cono de las comunicaciones o cesiones que se han realizado y de las que se prevean.

Es función del Responsable del fichero proporcionar toda esta información a los interesados de forma totalmente gratuita. La forma más sencilla de poder responder a una petición de acceso se consigue mediante la visualización en pantalla de esos datos. Pero también se puede responder a esta petición a través de un escrito, un correo electrónico, una copia, certificada o no, en forma legible, la cual no requiera el uso de mecanismos específicos.

Este derecho puede llevarse a cabo, sin justificación necesaria por parte del titular de los datos, a intervalos de 12 meses, pero por el contrario, si el titular quiere ejercer este derecho a intervalos inferiores, deberá acreditar el interés legítimo.
El Responsable del fichero resolverá la solicitud en el plazo máximo de un mes desde la recepción de la solicitud y el titular de los datos podrá acceder a ellos en el plazo de diez días desde la respuesta a su solicitud por parte del Responsable.
La no respuesta en el plazo marcado de un mes a la solicitud del ejercicio del derecho de acceso implica que se desestima la solicitud y por tanto se deberá informar al usuario.

Se podrá denegar el derecho de acceso en algunos casos puntuales. Es el caso de los ficheros de la Hacienda Pública o los datos de los ficheros que puedan suponer un peligro para la defensa del Estado o la seguridad pública.

- **Derecho de rectificación y cancelación**

Si una persona puede acreditar que una empresa tiene un fichero con datos personales suyos y que éstos son inexactos o están incompletos, entonces podrá solicitar al Responsable del fichero que rectifique esos datos.
Para ello deberá aportar la solicitud de rectificación, la cual debe contener los datos erróneos y la corrección que se debe realizar, y la documentación justificativa de lo solicitado

Del mismo modo, si una persona desea que se supriman datos personales inadecuados o excesivos o datos que cuya finalidad para la que fueron recabados haya finalizado, entonces podrá ejercer el derecho de cancelación. Al igual que en el ejercicio del derecho de rectificación, el titular debe aportar la solicitud correspondiente indicando a qué datos se refiere y adjuntando la documentación que lo justifique.

En el caso de la cancelación, el Responsable del fichero bloqueará, en vez de cancelar, los datos solicitados si es necesaria su conservación para fines de le Administraciones Públicas, Jueces y Tribunales de cara a posibles responsabilidades. Este bloqueo durará lo equivalente al plazo de prescripción de estas responsabilidades y una vez terminado este plazo, entonces se debe proceder a la supresión total de los datos. El bloqueo es el efecto derivado de la cancelación.
Si no es necesaria su conservación para los fines descritos, entonces se llevará acabo la cancelación de esos datos y eso implica un borrado físico de los datos.
Además, si se demuestra que los datos personales del afectado fueron recabados de forma fraudulenta, desleal o ilícita, la cancelación de los datos irá más allá y el Responsable del fichero estará obligado a destruir el soporte físico en el que estén esos datos.

En el caso que estos datos rectificados o cancelados hubieran sido cedidos a un tercero, el Responsable del fichero será el encargado de notificar esos cambios al cesionario, en idéntico plazo para que éste proceda también a modificar o cancelar los datos en el plazo de diez días a partir de la recepción de la comunicación.

Se denegarán las solicitudes de cancelación de datos en el caso de que exista un deber legal de su conservación, en el caso de que sean necesarios para las relaciones contractuales o en el caso que su cancelación pueda perjudicar al propio titular o a terceros.

Para ambos casos, el Responsable del fichero tiene un plazo máximo de 10 días para resolver dichas solicitudes.

También en el ejercicio de estos dos derechos, el Responsable del fichero deberá responder a las solicitudes recibidas ya tenga en sus ficheros datos personales del afectado o no.

- **Derecho de oposición**

Mediante el derecho de oposición, una persona puede oponerse al tratamiento de sus datos personales u oponerse a que sus datos sean comunicados a terceros, si no existe una ley que disponga lo contrario.
Este derecho se podrá ejercer sobre ficheros para los cuales no se necesita consentimiento o para ficheros que tengan fines comerciales y publicitarios.

Si el titular de los datos no dio su consentimiento para que se guardaran en un fichero, entonces se debe solicitar el derecho de oposición justificándolo con motivos fundados y legítimos. Así que se excluirán esos datos del tratamiento.

Si por el contrario, se los datos personales del afectado se encuentran en un fichero de carácter comercial, no se necesitan motivos para oponerse, simplemente se solicita al Responsable del tratamiento la oposición.
En este caso lo datos serán dados de baja del tratamiento de modo que se cancelarán todos los datos del afectado.

Este derecho se puede ejercitar en el momento de la recogida de los datos o posteriormente, dirigiendo la solicitud al Responsable del fichero o tratamiento.

Como en los demás derechos de los titulares de datos de carácter personal, hay excepciones. El derecho de oposición no puede ejercitarse en muchos ficheros de titularidad pública como son los de Hacienda Pública, los ficheros policiales y los de la Seguridad Social entre otros.

El plazo máximo para responder a las solicitudes es de un mes a contar desde la recepción de la petición. Se debe responder al afectado se tengan o no datos personales de él, y siempre a través de un medio sencillo y gratuito.

- **Tutela de los derechos**

Los interesados a los cuales se les deniegue, de forma parcial o total, el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, podrán comunicárselo a la AEPD o al organismo competente de cada Comunidad Autónoma, para que evalúe esta negación. Este procedimiento lo denominamos tutela de los derechos y su fin es garantizar el ejercicio efectivo de los derechos ARCO por parte de los ciudadanos.

Para hacer efectivas la solicitud de tutela de derechos, el afectado tendrá que presentar en la AEPD un escrito que contenga el contenido de su reclamación y los preceptos de la LOPD que considere vulnerados.
Una vez la AEPD recibe esta solicitud, permite al Responsable del fichero o tratamiento formular las alegaciones pertinentes y para ello le concede un plazo de quince días. Después de estos quince días, es la AEPD la que tiene un plazo de seis meses para resolver la reclamación.

Si el Responsable del fichero o del tratamiento no está de acuerdo con la resolución de la AEPD, deberá interponer un recurso potestativo de reposición o un recurso contencioso-administrativo ante la Audiencia Nacional.

La AEPD, mediante el procedimiento de tutela de los derechos, se limita a estimar o desestimar las reclamaciones de los afectados. Este procedimiento no tiene carácter sancionador, pero en ocasiones puede que se de lugar la iniciación de procedimientos sancionadores.
Este procedimiento se verá más adelante en el apartado "Infracciones y sanciones".

- **Derecho a indemnización**

Los titulares de datos de carácter personal que hayan sufrido daños o perjuicios debido al incumplimiento de la LOPD por parte del Responsable del fichero o tratamiento, podrán atenderse a su derecho de indemnización.

- **FICHEROS DE TITULARIDAD PÚBLICA Y FICHEROS DE TITULARIDAD PRIVADA**

Definimos el concepto de **fichero de titularidad pública** como aquellos ficheros cuyos responsables sean los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público. (Derecho.com, 1997).

Estos ficheros no podrán ser cedidos a otras Administraciones Públicas a no ser que sea para fines científicos, estadísticos o históricos. Pero sin embargo, queda totalmente prohibido ceder datos de ficheros de titularidad pública a ficheros de titularidad privada sin el previo consentimiento del titular de los datos.
En cuanto a las Fuerzas y Cuerpos del Seguridad del Estados, los ficheros que manejan con fines administrativos, también están sujetos a la normativa de la LOPD y éstos podrán recoger datos de carácter personal de personas sin el previo consentimiento, siempre y cuando sean necesarios para la prevención de un peligro para la seguridad pública o para la prevención de infracciones penales.

Del mismo modo y siguiendo con la misma fuente, definimos los **ficheros de titularidad privada** como los ficheros cuyos responsables son las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

Dentro del análisis de los ficheros de titularidad privada, encontramos los **Códigos Tipo** los cuales constituyen acuerdos sectoriales que establecen las condiciones de utilización de los ficheros de carácter personal en el entorno de la empresa que lo haya elaborado.
Se le atribuye un carácter deontológico o de buena práctica profesional. No obstante, estos Códigos no son obligatorios, sino que son de confección voluntaria.

A su elaboración se le atribuyen básicamente dos ventajas. Por un lado, la empresa en cuestión refleja ante los clientes una buena imagen ya que muestra un gran interés en el hecho de respetar los derechos de éstos. Y por otro lado, la empresa refleja también una buena imagen ante la propia Agencia de Protección de Datos ya que los Código Tipo se inscriben en el Registro General de Protección de Datos después de que la AEPD los examine y evalúe (protecciónlegal.com, 2005).

Para elaborar un Código Tipo, su empresa debe tener en cuenta, que según el artículo 72.3 del RDLOPD, el Código debe contener como mínimo los siguientes documentos:

-Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.

-Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.

-Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

-Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Cuando esté elaborado el Código Tipo, se debe inscribir en el RGPD y tal como se ha comentado antes, para que sea examinado con el fin de ajustarse a las disposiciones legales de la normativa.

- **INSCRIPCIÓN DE FICHEROS**

Una de las normas básicas que establece la LOPD, es la adaptación legal de los ficheros de las empresas, ya sean automatizados, no automatizados o mixtos. Esto implica que todas las empresas deben notificar sus Ficheros de carácter personal en la Agencian Española de Protección de Datos.
Para llevar esto a cabo, su empresa debe de determinar todos los ficheros que ya existan, así como determinar los ficheros que se deseen crear.
Por este motivo, le aconsejamos que para una buena determinación, realice un inventario de todos sus ficheros preexistentes. Para una buena clasificación debe tener en cuenta una serie de información como el origen de los datos que son tratados, la finalidad de dicho tratamiento y los tratamientos que se les hayan realizado.

De los dos tipos de ficheros definimos en el punto anterior, los de titularidad pública y los de titularidad privada, nosotros no centraremos más en los privados ya que nuestra empresa es privada, pero no por ello dejaremos de hablar de los públicos.

El artículo 20 de la LOPD regula la *"Creación, modificación o supresión"* de los ficheros de titularidad pública e indica que para la creación de un fichero de

titularidad pública es necesaria la aprobación de una disposición general o acuerdo publicado en el Boletín Oficial del Estado (BOE) o en el diario oficial correspondiente. En este mismo artículo se detalla el contenido de dicha disposición o acuerdo:

- Finalidad y usos del fichero
- Personas sobre las que se pretendan obtener datos de carácter personal y el procedimiento de recogida de estos datos
- Estructura del fichero, el tipo de datos que contendrá
- Las cesiones de datos de carácter personal y las transferencias que se vayan a realizar
- La Administración responsable del fichero
- Las medidas de seguridad con indicación del nivel exigible

El órgano competente de la Administración responsable del fichero público que se desea inscribir tiene 30 días, desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente, para notificarlo a la Agencia Española de Protección de Datos.

En cuanto a los ficheros de titularidad privada, que se regulan en el artículo 25 de la LOPD, se pueden crear siempre que sean necesarios para lograr una actividad u objetivo de la empresa en cuestión, pero siempre teniendo en cuenta que se deben respetar las garantías de protección que establece la LOPD para todos los nuevos ficheros.
En este caso, será la persona o entidad privada que quiera crear el fichero de titularidad privada quien tenga que notificarlo a la Agencia Española de Protección de Datos y lo debe de notificar antes de su propia creación.
Esta notificación, según el artículo 26 de la LOPD, deberá contener 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".*

Así que una vez localizados y determinados los ficheros de carácter personal, se notifican a la AEPD para que ésta los inscriba. Añadir también que la posterior modificación o supresión de ficheros implica, del mismo modo, tener que notificarlo ante el RGPD. A continuación vamos a detallar los pasos para una correcta notificación.

El proceso de notificación es totalmente gratuito y se debe realizar a través de una aplicación creada por la AEPD que contiene el Formulario aprobado por Resolución de 30 de Mayo de 2000.
Dicha aplicación llamada NOTA (Notificaciones Telemáticas de la Agencia) se puede descargar directamente a su equipo desde la página web de la Agencia Española de Protección de Datos, www.agpd.es. La misma aplicación le va guiando de los pasos a seguir y además es muy recomendable leer primero los diversos manuales de ayuda que podrá encontrar en la misma página web.

En el "Manual del Formulario Electrónico de Notificación de Ficheros de Titularidad Privada" disponible en la página web de la AEPD, encontramos resumidos los pasos a seguir para cumplimentar el formulario (en el manual original se explican con más detalle):

1. Responder a las preguntas iniciales del asistente dependiendo del tipo de solicitud y forma de presentación elegido.

2. Cumplimentar los apartados de la notificación.

3. Cumplimentar la Hoja de solicitud.

4. Generar/Enviar la notificación.

5. En las presentaciones a través de Internet, deberá recibir el acuse de recibo de la AEPD del envío realizado. La no recepción del mensaje de confirmación, o en su caso, la recepción de una mensaje de indicación de error implica que no se ha producido la recepción del mismo, debiendo realizarse la presentación en otro momento o utilizando otros medios.

6. Enviar la *Hoja de solicitud* a la AEPD.

Cuando la Agencia de Protección de Datos recibe la notificación de fichero y la solicitud de inscripción, se evalúa la información y si todo es correcto se inscribe el Fichero pero si el resultado de la evaluación es que hay algún error, entonces se solicita al Responsable del Fichero que los corrija.
Una vez inscrito, la AEPD le facilitará al Responsable del fichero, el código de inscripción asignado a dicho fichero. Es muy importante conservar el código de inscripción ya que es necesario para realizar modificaciones en el fichero o para suprimirlo. Estas dos acciones también se deben efectuar a través de la aplicación NOTA por parte del Responsable del Fichero.

- **FICHEROS TEMPORALES**

Una de las novedades en la LOPD respecto a la LORTAD, es el establecimiento de ficheros temporales.
Realmente, en el texto normativo de la LOPD no se concreta ninguna definición para este nuevo concepto, sólo se encuentra una única referencia en el RD 994/1999 de Medidas de Seguridad que estable las medidas que deberán ser adoptadas para la protección de este tipo de ficheros (Microsoft, 2009).
La definición dada por un abogado especialista en derecho informático, es que se trata de aquellos ficheros o bases de datos que se crean para un tratamiento ocasional, es decir limitado en el tiempo, o como paso intermedio durante la realización de un tratamiento (Xavier Ribas, 2008)

Estos ficheros deben también necesariamente inscribirse en la Agencia Española de Protección de Datos e informar a la misma de la modificación o supresión.

Pero tal y como se comenta en una guía Práctica de Adaptación de la LOPD elaborada por Microsoft, puede haber excepciones en los casos de creación de ficheros de acciones muy concretas y plazos muy cortos de tiempo como por ejemplo la extracción de datos de la base de datos corporativa a través de la impresión de listados, con el fin de realizar un mailing y facilitar la labor de las personas encargadas de preparar el mismo (Microsoft, 2009).

Además, a estos ficheros temporales también se les debe implantar unas adecuadas medidas de seguridad, las cuales se hallarán en el Documento de Seguridad de la empresa, el cual trataremos más adelante.

Los ficheros temporales provocan problemas en las empresas ya que no se sabe con exactitud los límites entre los ficheros temporales y el resto de los ficheros, de modo que para una correcta ejecución de la normativa de protección de datos, se debe de formar a los trabajadores de la empresa en cuestión para no violar la LOPD.

- **MOVIMIENTO INTERNACIONAL DE DATOS**

Se denomina movimiento internacional de datos o transferencia internacional de datos a cualquier transmisión de datos de carácter personal, con independencia del medio y soporte del envío, fuera del territorio español.

Se diferencian dos casos en las transferencias internacionales: transferencias de datos a países con un nivel de protección adecuado, y transferencias de datos a países con un nivel de protección inadecuado.

Consideramos países con un nivel de protección adecuado a los miembros del Espacio Económico Europeo, Islandia, Liechtenstein, Noruega o un Estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que garantiza un nivel de protección adecuado.

El resto de los países del mundo se consideran países con un nivel de protección inadecuado y si se quiere realizar una transferencia a uno de ellos, es necesario que se obtenga la autorización del Director de la AEPD.
Esta autorización sólo se podrá otorgar si se obtienen garantías adecuadas y se debe pedir a través de una solicitud por parte del exportador de datos. Éste deberá explicitar la finalidad de la transferencia, los datos que se van a transferir, los interesados y la documentación necesaria para acreditar las garantías de la protección de datos por parte del importador de los datos. Además se deben incluir unas medidas de seguridad que serán adoptadas tanto por el exportador como por el importador de los datos.

Además de la autorización, el Responsable de fichero debe cumplir con la LOPD y por eso deberá informar sobre la cesión de datos o sobre el acceso a datos por cuenta de terceros a los afectados. También notificará de la transferencia a la AEPD para su inscripción en el Registro General de Protección de Datos, indicando el país al que se pretende realizar la transferencia y la categoría del destinatario.

No será necesaria esta autorización si la transferencia en cuestión está incluida en las excepciones del artículo 34 de la LOPD. Algunas de las posibles excepciones son: tratados o convenios, auxilio judicial internacional, transferencias dinerarias, contrato entre el titular de los datos y el responsable del fichero, contrato entre el responsable del fichero y un tercero, etc.

Si estas indicaciones no se cumplen y se realiza una transferencia temporal o definitiva de datos personales a un país que no proporciona un nivel de protección adecuado y sin autorización del Director de la AEPD, entonces se constituirá una falta muy grave.

- **AGENCIA DE PROTECCIÓN DE DATOS**

A lo largo de toda esta guía se insiste en lo importante que es que un empresario como usted proteja todos los datos de carácter personal que necesite para el desarrollo de su actividad empresarial. Por ello se instauraron las Agencias de Protección de Datos.

A nivel nacional, en nuestro país contamos con la Agencia Española de Protección de Datos (AEPD) que fue creada en 1994 para velar por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal.
Esta Agencia es un ente de Derecho Público que cuenta con personalidad jurídica propia y la cual cuenta con una plena capacidad pública y privada. Además, actúa con total independencia de las Administraciones Públicas y su ámbito de actuación se extiende a toda España.

Básicamente las funciones de la AEPD se pueden resumir en cuatro. Una de las funciones es la de informar sobre el contenido, los principios y las garantías del derecho a la protección de datos tal y como se regula en la LOPD. Otra función es la de ayudar a ejercer los derechos de los ciudadanos, y con estos derechos nos referimos a los derechos de información, acceso, rectificación, oposición y cancelación de datos. Además, también se ofrece ayuda a los responsables y encargados de tratamiento de datos. Y por último, la agencia centra su atención en requerir medidas de corrección, investigar actuaciones que puedan ser contrarias a la ley y en consecuencia ejercer la potestad sancionadora sobre éstos que cometen las irregularidades.

El 20% de la actividad de la AEPD se dedica a la acción preventiva, es decir a la orientación y sensibilización sobre el cumplimiento de la LOPD en los distintos sectores de la sociedad; mientras que el 80% de los recursos de la Agencia son dedicados a acciones reactivas, como por ejemplo la tramitación de quejas, a la imposición de sanciones, etc.

Para llevar a cabo sus tareas, la AEPD cuenta con unos elementos claves. Uno de ellos es el hecho de contar con competencias y poderes efectivos de investigación legales. Además, dispone de recursos humanos con un adecuado nivel técnico, así como de expertos legales los cuales trabajan juntos en la cooperación permanente. Por otro lado, cuenta con unos factores de organización que implican la definición de roles y responsabilidades entre los inspectores y la formación de éstos.

Pero el elemento más significativo es la especialización por parte de la AEPD en el desarrollo de auditorías en todos los sectores y para el desempeño de las éstas se busca como interlocutor en la empresa auditada a una persona de contacto de alto nivel (European Data Protection Supervisor, 2007)

Por otra parte, Madrid, Cataluña y País Vasco cuentan con agencias de protección de datos de carácter autonómico que actúan sobre los ficheros públicos que existen esas comunidades autónomas.

No sólo España cuenta con una Agencia de Protección de datos, sino que todos los países de la Unión Europea han constituido una, y también otros países de los cinco continentes.
Otros muchos países están todavía en vías de desarrollo de esta clase de leyes y otros tantos aún tardarán muchos años en instaurar una ley tan fundamental de estas características.

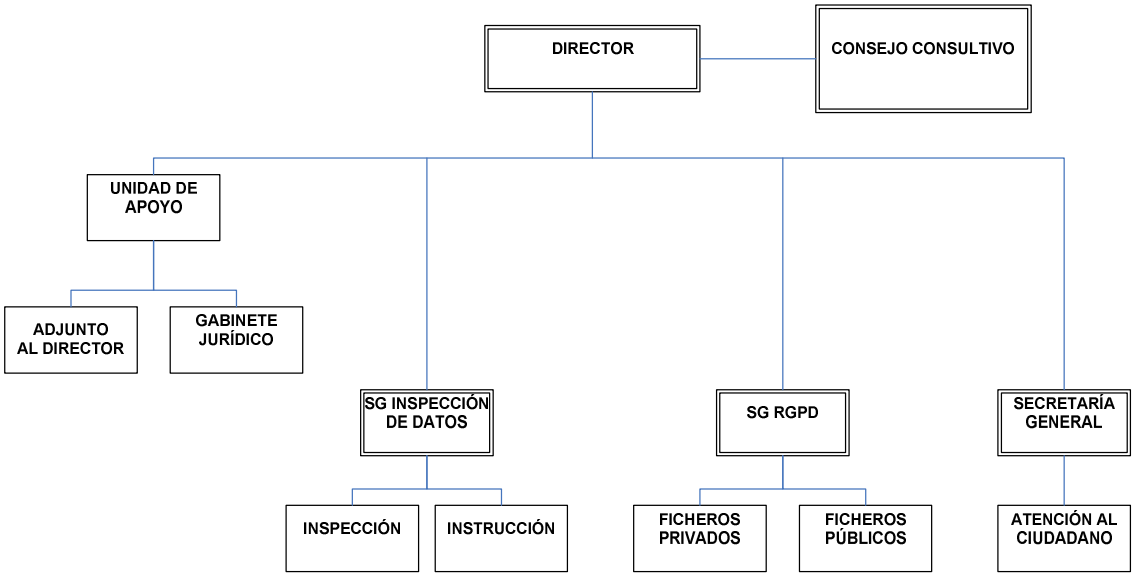
En cuanto a la estructura de la AEPD, ésta cuenta con un Director que será su representante. La función fundamental del Director es establecer resoluciones sobre inscripciones, códigos tipo, transferencias, tutelas de derechos, procedimientos sancionadores y medidas cautelares entre otros.

Este Director estará asesorado y será elegido de entre los miembros de un Consejo Consultivo el cual está formado por diversos representantes de diversas instituciones y órganos de gobierno como son por ejemplo un senador propuesto por el Senado o un experto en la materia, propuesto por el Consejo Superior de Universidades.

Otro órgano que integra la Agencia es el Registro General de Protección de Datos. En este Registro se deberán inscribir todos los ficheros tanto de titularidad pública como privada, las autorizaciones a que se refieren la LOPD, los códigos tipo, así como los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición. La función del Registro es velar por la publicidad de los datos.

Siguiendo con la estructura de la Agencia, encontramos la Inspección de Datos, cuya función es la comprobación de la legalidad de los tratamientos, y la Secretaría General de la Agencia, que tiene como función dar apoyo a la Agencia para un adecuado funcionamiento de ésta.

A continuación se muestra el organigrama de la Agencia Española de Protección de Datos obtenido de la página web www.agpd.es.



- **INFRACCIONES Y SANCIONES**

La AEPD, representada por su Director, podrá iniciar un procedimiento sancionador contra los Responsables o Encargados de los ficheros en el caso en que se produzca alguna violación de los principios y garantías que expone la LOPD y haya pruebas claras de estos hechos.

Este procedimiento se inicia si algún titular de datos de carácter personal denuncia ante la AEPD cualquier irregularidad cometida sobre sus datos o si la propia AEPD es sabedora de algún hecho ilícito.

La AEPD es la responsable de investigar los hechos denunciados y si lo ve conveniente tiene autoridad para suspender temporalmente el tratamiento de esos datos. La AEPD ordenará la supresión o destrucción de los datos o prohibirá el tratamiento si después de la investigación realizada, se demuestra que realmente se han tratado datos de forma ilícita.

Además, las infracciones cometidas se saldarán con sanciones económicas. Esta cuantía dependerá de la gravedad de la infracción, de 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 otras circunstancias que resulten relevantes.

Las infracciones se clasifican en tres tipos: leves, graves o muy graves.

En el artículo 44 se enumeran estas infracciones.

- **Infracciones leves:**

  - No atender la solicitud del interesado de rectificación o cancelación de los datos sujetos a tratamiento cuando proceda legalmente.

  - 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.

  - 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.

  - Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la LOPD.

  - Incumplir el deber de secreto establecido en el artículo 10 de la LOPD, salvo que constituya infracción grave.

- **Infracciones graves**:

  - 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.

  - 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.

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

  - Tratar los datos de carácter personal o usarlos posteriormente infringiendo los principios y garantías establecidos en la LOPD o con el incumplimiento de los mandatos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituye infracción muy grave.

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

  - 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 LOPD ampara.

  - 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.

- 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.

- No remitir a la Agencia de Protección de Datos las notificaciones previstas en la LOPD 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.

- La obstrucción al ejercicio de la función inspectora.

- No inscribir el fichero de datos de carácter personal en el Registro General de Protección de 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 la LOPD, cuando los datos hayan sido recabados de persona distinta del afectado.

- **Infracciones muy graves:**

  - La recogida de datos en forma engañosa y fraudulenta.

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

  - Recabar y tratar los datos de carácter personal 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 articulo 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.

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

  - La transferencia temporal o definitiva de datos de carácter personal 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.

  - 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.

- 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 de la LOPD, 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 de la inclusión de datos de carácter personal en un fichero

- **Sanciones**

Las infracciones leves prescriben al año y la cuantía a pagar en caso de cometer una se sitúa entre los 600 y los 6000 euros.
Las infracciones graves prescriben a los dos años y varían entre 60000 y 300000 euros.
Mientras que las infracciones muy graves prescriben a los tres años y la cuantía a pagar varía entre 300000 y 600000 euros.

DOCUMENTO DE SEGURIDAD

- **MEDIDAS DE SEGURIDAD**

Todas las empresas que traten con datos de carácter personal deben establecer unas medidas de seguridad las cuales garanticen la seguridad, la confidencialidad, la integridad y la exactitud de los datos de carácter personal y eviten la alteración, pérdida, tratamiento o acceso no autorizado de éstos.
Estas medidas de seguridad son establecidas por el Real Decreto 994/1999 por medio de la aprobación del Reglamento de Medidas de Seguridad para los Ficheros automatizados de Datos de Carácter Personal.

Las medidas de seguridad exigibles tanto a los ficheros como a los tratamientos de datos personales se clasifican en tres niveles: básico, medio y alto. Esta clasificación viene dada por el carácter y tipo de datos de los ficheros o tratamientos. Cuanto mayor es el nivel de sensibilidad, mayores y más estrictas son las medidas a aplicar para proteger los datos. Por eso, estos niveles de seguridad son acumulativos. El nivel medio abarca también las medidas previstas para el nivel básico y del mismo modo el nivel alto abarca las medidas previstas tanto en el nivel básico como en el medio.

- **Nivel básico**

En este nivel se encuentran todos los ficheros o tratamientos que contienen datos de carácter personal. También se consideran de nivel básico los que contienen datos de ideologías, afiliación sindical, religión, creencias, salud, origen racial o vida sexual siempre y cuando estos datos se utilicen para realizar transferencias monetarias a entidades de las que los afectados son miembros, o siempre que se trate de ficheros o tratamientos no automatizados o manuales y que no guarden relación con la finalidad del fichero, o en el caso de contener datos de salud referidos al grado o condición de discapacidad, con motivo del cumplimiento de deberes públicos (“Guía de Seguridad de Datos”, AEPD).

A este nivel de seguridad son aplicables todas las medidas del Documento de Seguridad referidas a los artículos 5 al 14 del Reglamento de la LOPD.

- **Nivel medio**

En este caso, se trata de todos los ficheros o tratamientos que contengan datos relativos a la comisión de infracciones administrativas o penales, a Hacienda Pública, a servicios financieros, a entidades gestoras y servicios comunes de Seguridad Social, a mutuas de accidentes de trabajo y enfermedades profesionales, a datos que ofrezcan una definición de las características o personalidad de los ciudadanos y permita evaluar aspectos de sus personalidad o comportamiento y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).

Son aplicables todas las medidas del Documento de Seguridad referidas a los artículos 5 al 22 del Reglamento de la LOPD.

- **Nivel alto**

  En este nivel se establecen todos los ficheros o tratamientos que contienen datos de ideología, religión, creencias, origen racial, salud y vida sexual para los cuales no se puede adoptar el nivel básico. Y además, los derivados de actos de violencia de género o los recabados para fines policiales sin consentimiento del afectado.

  Son aplicables todas las medidas del RDLOPD referidas a los artículos 5 al 26.

Los plazos para la implantación de las medidas de seguridad de estos tres niveles ya han vencido, de modo que toda empresa debe tenerlas ya establecidas en su organización.

Tal y como se expone en la Guía Práctica de Adaptación de la LOPD de Microsoft, todas las empresas pueden establecer las medidas correspondientes para ficheros de nivel básico y algunas de las medidas de nivel medio sin incurrir en grandes inversiones económicas ya que por ejemplo todos los equipos informáticos que podemos encontrar hoy en día en el mercado incorporan herramientas que permiten generar copias de seguridad, y también porque los sistemas operativos y las aplicaciones informáticas permiten a los usuarios configurar el control de acceso, los controles de seguridad, la implantación de perfiles y los sistemas de autenticación.

- **DOCUMENTO DE SEGURIDAD**

Según dictamina la AEPD en su "Guía se seguridad de datos", el Documento de Seguridad es *"un documento interno de la organización, que debe mantenerse siempre actualizado. Disponer del documento de seguridad es una obligación para todos los responsables de ficheros y, en su caso, para los encargados del tratamiento, con independencia del nivel de seguridad que sea necesario aplicar."*.

Éste recoge todas "*las medidas de índole técnica y organizativa necesaria para garantizar la protección, confidencialidad e integridad*" de los datos personales tratados por una empresa en cuestión.
Con medidas técnicas nos referimos a las medidas que se establecen primordialmente para conservar la integridad de la información y los sistemas de información, los ficheros, los locales, los equipos y los restantes elementos materiales que tratan datos, son los destinatarios de esta clase de medidas.
En cambio, las medidas organizativas son las destinadas a elaborar procedimientos, normas, reglas y estándares de seguridad y los usuarios que tratan estos datos de los ficheros son los destinatarios de estas medidas.

Quedan excluidos del ámbito de aplicación de ambos tipos de medidas los fichero en soporte papel los cuales hayan sido creados antes de la LOPD entrara en vigor, los ficheros automatizados que no contengan datos personales y los ficheros automatizados que sean de uso personal y/doméstico.

Este Documento protege los datos de carácter personal y toda modalidad de uso o tratamiento de los mismos, es decir la recogida, grabación, conservación,

elaboración, modificación, consulta, utilización, modificación, cesión o transmisión de los datos, y también los protege en caso de que se produzcan incidencias, fallos o actuaciones malintencionadas por parte de terceros.
Recalcar también, que se presta una especial atención a la protección de los datos desde el propio ámbito interno de la empresa como pueden ser medidas para restringir el acceso a cierta documentación a determinados empleados o la firma de cláusulas de confidencialidad por parte de los empleados (Microsoft, 2009).

A parte de mantenerlo siempre actualizado, deberá ser siempre revisado cuando se produzcan cambios relevantes en los sistemas de información, en la organización de los mismos o en la normativa aplicable.

Las empresas pueden optar por disponer de un solo Documento de Seguridad, en el cual se incluyan todos los ficheros y tratamientos de datos de carácter personal de los que una persona, ya sea física o jurídica, sea responsable, o puede optar por disponer de un Documento de Seguridad por cada fichero o tratamiento que atiendan a los criterios organizativos que el responsable establezca.

Tal y como expone el artículo 88.3 del RDLOPD y la guía "Guía para empresas: cómo adaptarse a la normativa sobre la protección de datos", el Documento de Seguridad debe incluir como mínimo los siguientes apartados:

-"*Ámbito de aplicación del documento con especificación detallada de los recursos protegidos*", es decir todos los ficheros que contengan datos de carácter personal los cuales estén bajo la responsabilidad de la empresa, y además se incluyen los sistemas de información, los soportes y los equipos empleados para el tratamiento de éstos, así como a las personas que intervienen en el tratamiento y los locales en los que se ubican.

-"*Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el reglamento*".

-"*Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros*".

-"*Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan*".

-"*Procedimiento de notificación, gestión y respuesta ante las incidencias*".

-"*Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados*".

-"*Las medidas que sean necesarias adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos*".

Además, para las medidas de seguridad de nivel medio y alto, se deberán incluir en el Documentos de Seguridad dos apartados más:

-"*Identificación del responsable o responsable de seguridad*".

-"*Los controles periódicos que se deban realizar para verificar el cumplimiento de los dispuesto en el propio documento*".

Puede que usted haya contratado la prestación de servicios por terceros para algunos de los ficheros, en este caso el Documento de Seguridad deberá contener una referencia al contrato, su vigencia y los ficheros implicados.

Por otra parte, si la prestación de servicios por terceros se realiza para la totalidad de los ficheros de su empresa y sus tratamientos y estos servicios se prestan en las instalaciones del encargado del tratamiento, entonces usted podrá delegar en éste la aplicación del Documento de Seguridad.

- **FUNCIONES Y OBLIGACIONES DEL PERSONAL**

Cualquier empleado de su empresa que tenga acceso a ficheros de datos de carácter personal deberá conocer todas las medidas de seguridad que se incluyan en el Documento de Seguridad que haya elaborado y que guarden relación con las tareas realizadas por éste. Además de los empleados de su empresa, también deberá informar a todo el personal externo a la empresa que le presten servicios y que para llevar a cabo estos servicios hagan uso de los ficheros de datos personales.
Por ello, la empresa debe informarles sobre la normativa de seguridad respecto a la protección de datos y sobre las consecuencias y sanciones en el caso de incumplimiento.

En el caso de que se traten en la empresa ficheros de nivel medio y alto, se definirá la figura del Responsable de Seguridad y tiene que aparecer identificado en el Documento de Seguridad. Éste es el encargado de coordinar y controlar las medidas de seguridad que se han definido en el citado Documento.

Tal y como expone el Instituto Nacional de Tecnologías de la Comunicación en una guía elaborada para facilitar la adaptación de las empresas a la normativa sobre protección de datos, las funciones del Responsable de Seguridad son las siguientes:

-Recopilar y describir las medidas, normas, procedimientos, reglas y estándares de seguridad adoptados por la empresa.

-Determinar el ámbito de aplicación del Documento de Seguridad.

-Establecer y comprobar la aplicación de las normas y procedimientos del Documento de Seguridad, entre otros, los procedimientos de notificación, tratamiento y registro de incidencias, de realización de copias de respaldo y recuperación de datos, de identificación y autentificación de usuarios, de asignación, distribución y almacenamiento de contraseñas, de cambio periódico de las contraseñas de los usuarios, de gestión de los soportes.

-Elaborar y mantener actualizada la lista de usuarios que tenga acceso autorizado al sistema informático de la empresa, con especificación del nivel de acceso que tiene cada usuario. Establecer y comprobar la aplicación de un sistema que

limite el acceso de los usuarios únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones y autorizados por el Responsable del Fichero.

-Velar por el cumplimiento de las normas de seguridad contenidas en el Documento de Seguridad.

Muchas de estas funciones serán ampliadas en los apartados sucesivos.

Podemos hacer una clasificación aproximada de las personas que se verán afectadas por sus normas de seguridad. Decimos aproximada porque según el tamaño de su empresa o según su organización, estos roles pueden variar.

En primer lugar tenemos al Responsable del Fichero, que suele ser el responsable de la empresa y el cual decide sobre la finalidad, contenido, uso y tratamiento de los ficheros que contienen datos de carácter personal.

Por otra parte tenemos al Responsable de Seguridad el cual hemos definido anteriormente. Puede que el Responsable del Fichero y el Responsable de Seguridad sean la misma persona, o puede que el Responsable del Fichero haya designado esta función a otro miembro de la organización. No obstante, en ningún caso esta designación eximirá al Responsable del Fichero de su responsabilidad ante el fichero.

Además contamos con los operadores, técnicos y administradores del sistema, los cuales son los encargados de administrar o mantener el entorno operativo de la información contenida en los ficheros y del acceso a los mismos. También se encargan de controlar los soportes y a todas las personas que generen, traten o gestionen soportes.

Y finalmente encontramos a los usuarios del fichero que son quienes usualmente hacen uso de los archivos físicos o del sistema informático de acceso a los ficheros.

Tanto el personal interno de la empresa, como el personal externo que haga uso de los ficheros con datos de carácter personal, están obligados a notificar al Responsable del Fichero o al Responsable de Seguridad sobre cualquier incidencia de la cual tenga constancia respecto a los recursos protegidos.
Otras responsabilidades comunes a todos estos usuarios es el de guardar secreto y confidencialidad sobre los datos personales que conozcan durante el desarrollo de sus respectivos trabajos y no revelar sus contraseñas, entre otras. Cada empleado debe acceder exclusivamente a los datos y recursos que precise para el buen desarrollo de sus actividades (Registradores de España).

- **NORMAS Y PROCEDIMIENTOS DE SEGURIDAD**

A continuación se van a describir las normas, medidas y procedimientos establecidos para garantizar los niveles de seguridad que se exigen en el Documento de Seguridad creado por la empresa. Las distintas medidas que se describen en los

puntos sucesivos han sido recopiladas de diferentes guías especializadas en la LOPD que se citan en la bibliografía, así como del Reglamento de Desarrollo de la LOPD.

Una norma es una *"regla de seguridad de obligado cumplimiento por ser un requerimiento legislativo o bien por ser una normativa de seguridad"* de la empresa en cuestión.

Estas normas y procedimientos de seguridad deben proteger todos los recursos que directamente o indirectamente permiten un acceso a los ficheros que contienen datos de carácter personal. De modo que los recursos protegidos básicamente son los que se citan en la "Guía para empresas" elaborada por el Instituto Nacional de Tecnologías de la Comunicación (INTECO, 2009):

-Los centros de tratamiento y locales donde se ubican los ficheros o los soportes que los contengan.

-Los puestos de trabajo, ya sean locales o remotos, desde los cuales se puede tener acceso a los ficheros.

-Los servidores, en el caso de haberlos, y el entorno de sistema operativo y de comunicaciones donde se ubican los ficheros.

-Los sistemas informáticos o aplicaciones que se hayan establecido para acceder a los datos.

- **Identificación y autenticación**

Definimos la identificación como el procedimiento por el cual un sistema de información reconoce a un usuario que trata con datos de carácter personal. Esto se produce a través del nombre de usuario que se le asigna a cada usuario del sistema.
Y la autenticación es el procedimiento por el cual se comprueba la identidad del usuario en el sistema, en decir, se comprueba que la contraseña de acceso dispuesta por el usuario está asociada al nombre de usuario del mismo.

Para este mecanismo, la empresa puede aprovechar los medios disponibles dentro de los sistemas operativos como los paquetes de control de acceso, que por ejemplo permiten crear diferentes cuentas cada una con su propia contraseña. Esta opción es más barata y presenta menos vulnerabilidades que contratar un sistema propio a una empresa de aplicaciones informáticas.

<u>Medidas de seguridad de nivel básico:</u>

-Cada usuario debe tener su propio identificador para cada servidor, base de datos o aplicación a la que necesite acceder.

-Los usuario no deben utilizar ningún identificador de otro usuario aunque dispongan de la autorización del propietario.

-Todo el personal debe tener conocimiento de las políticas y normativa de seguridad respecto de la utilización de contraseñas.

-Todos los usuarios deberán tener asignada su correspondiente contraseña. No se permitirán en ningún caso usuarios sin contraseñas.

-Los sistemas deben disponer de un mecanismo que permita autenticar la identidad de los usuarios.

-Los usuario no deben revelar bajo ningún concepto su contraseña a otra persona, siendo responsables de toda actividad relacionada con su uso. Ni siquiera el personal técnico debe tener conocimiento de esta información. Sólo en casos muy justificados se permitirá esta revelación.

-En caso de que la contraseña sea conocida fortuita o fraudulentamente por personas no autorizadas y comprometa su confidencialidad o el usuario tenga sospecha de su compromiso, éste deberá proceder inmediatamente a su cambio y ser comunicada al administrador quien deberá registrarlo como incidencias y tomar las medidas oportunas, si procede. Además, los usuarios serán las responsables de cambiar sus contraseñas con la periodicidad que se fije en cada entorno. La nueva contraseña nunca podrá ser igual a la anterior.

-Únicamente las personas autorizadas deberán tener acceso a los ficheros que contienen las contraseñas cifradas.

-Las contraseñas son confidenciales y privadas.

-Los sistemas deben almacenar las contraseñas de identificación de manera no inteligible.

-Los usuario y contraseñas deberán ser comunicados de forma segura, especialmente en los casos de asignación inicial de contraseñas o cuando un usuario la olvida y es necesario el cambio de la misma por parte de los administradores.

-La comunicación se realizará bien en persona o mediante otro método que garantice la confidencialidad e integridad del envío.

-Existirá un procedimiento o mecanismo seguro para la asignación y distribución de las contraseñas iniciales.

<u>Medidas de seguridad de nivel medio:</u>

-Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

- **Control de acceso**

El control de acceso regula las autorizaciones que poseen los usuarios para acceder a los recursos.
El acceso a los recursos dentro de una empresa debe estar restringido y autorizado.
Para ello se definen unos privilegios de acceso según la categoría funcional o jerárquica del usuario.
Dentro del control de acceso, podemos diferenciar entre acceso lógico y acceso físico.

Primero trataremos el acceso lógico que contempla todos los accesos a los recursos informáticos y documentales dentro de la empresa.
Las principales funciones del control de acceso lógico son controlar y proteger los accesos a la información, evitar delitos informáticos y evitar robos de material, de programas o equipos, evitar accesos no autorizados a los sistemas de información, así como asegurar la seguridad de la información (Bernal y Coltell 1996:285).

Hay múltiples personas que podrían realizar un acceso lógico no autorizado: los usuarios finales, el personal a tiempo parcial o temporal, los proveedores y consultores externos sin permisos de acceso a determinada información, ex-empleados, terceros interesados y piratas informáticos.

El control lógico más usado es la autenticación la cual puede realizarse a través de contraseñas, firma electrónica u otros métodos más avanzados como los biométricos. Lo importante del sistema a utilizar es que sean aplicables, prácticos y rentables.

Medias de seguridad de nivel básico:

-Deberá existir una relación actualizada de usuarios con acceso autorizado al sistema de información, con procedimientos de identificación y autenticación para dicho acceso.

-Los sistemas deben verificar los derechos de acceso del usuario, con el fin de identificar los recursos a los que pretenda acceder.

-Los sistemas deberán asegurar que los usuarios no acceden a determinados recursos a los que no tienen permiso de acceso.

-Exclusivamente el personal autorizado podrá conceder, alterar o anular el acceso autorizado, conforme a los criterios establecidos por los responsables de los datos.

-Los sistemas de información deben disponer de un mecanismo para inhabilitar usuarios que dejen de estar autorizados a utilizar dichos sistemas.

-Los sistemas deben permitir dar de baja a los usuarios así como volverlos a dar de alta tras un período de tiempo.

-En el caso de que existiera personal ajeno al Responsable del Fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Medidas de seguridad de nivel alto:

-En los accesos a los datos de los ficheros automatizados se registrará por cada acceso: la identificación del usuario, fecha y hora del acceso, fichero al que se ha accedido, tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso sea autorizado, se registrará también la información que permita identificar el registro accedido. El registro se llevará a cabo en soporte electrónico.

-En los accesos a los datos de los ficheros no automatizados se registrará por cada acceso la misma información que en el caso de ficheros automatizados. Este registro se llevará a cabo también en soporte electrónico.
Además se deberá mantener también una lista actualizada de los usuarios con acceso físico a las ubicaciones de tratamiento de ficheros o archivos.

-Los sistemas deben asegurar que los intentos de acceso no autorizados a cualquier recurso puedan ser identificados y supervisados, recogiendo la mayo cantidad de información relevante.

-El Responsable de Seguridad deberá revisar cada mes los accesos e intentos de acceso a los sistemas.

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

Pasando ahora a tratar el acceso físico, según el artículo 99 del RDLOPD, *"exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información."*

Entre los objetivos primordiales del control físico encontramos la evitación de accesos no autorizados al área no pública de la empresa, de daños contra la información que esté ubicada en los locales de la empresa y de daños contra los ordenadores y dispositivos que contengan información de la empresa.

El acceso físico no autorizado puede deberse a la falta de protección física del edificio, puertas y ventanas de nuestra empresa, a un uso inadecuado de los propios controles físicos o a una formación insuficiente del personal sobre seguridad. Y puede afectar a la información, al tratamiento de esta, a las infraestructuras o al hardware.

Con el fin de controlar el acceso físico la empresa debe implantar una serie de medidas de seguridad. Si se trata de una empresa pequeña podemos hacer uso de carteles donde se indique que se prohíbe el paso al personal ajeno, pero esta medida no es muy efectiva de modo que podemos hacer uso de métodos más elaborados como el acceso mediante contraseña, las tarjetas magnéticas que los usuarios deben pasar por un lector para acceder a una ubicación restringida, o un sistema de huellas digitales o reconocimiento de voz. (Rueda, 2003:61)
Además se puede hacer uso de cámaras y vigilantes y de otras medidas para evitar pérdidas por accidentes o producidas por desastres.

En el caso de que personas ajenas a la empresa tengan que entrar en las instalaciones de esta, deberían ser acompañadas por un miembro de la plantilla de la empresa en todo momento o al menos facilitarles una acreditación o tarjeta de acceso y unas condiciones de uso las cuales debe firmar.

Muchas empresas, generalmente las grandes, recurren cada vez más a instaurar un Responsable del control de acceso físico como pueden ser las empresas de seguridad

externas. En este caso sería la empresa de seguridad la encargada de llevar a cabo el registro de acceso de las visitas.

Entre las medidas a instalar más sofisticadas para asegurar la seguridad durante las horas de cierre en la empresa citamos las siguientes: detectores de infrarrojos, audio detectores, barreras de microondas, barreras luminosas o sensores de movimiento. Pero estas medidas requieren un gran desembolso económico y las pequeñas empresas no pueden permitírselo.
En cambio, las pequeñas empresas si que podrían acceder a instalarse alarmas, las cuales detectan a los intrusos y avisan de un acceso indebido, así como también cámaras de video-vigilancia en el exterior de sus locales. Otro método accesible para las pequeñas empresas es la instalación de rejas en ventanas a nivel de calle y de puertas dotadas de sistemas de seguridad.

Como ya se ha dicho, uno de los objetivos del control de acceso físico es evitar daños en el sistema de información así como en todos los soportes que contengan información, de modo que se ha de poner especial atención en las amenazas provinentes de los desastres naturales, incendios e inundaciones. Para ello debería estar la zona de almacenamiento perfectamente definida y controlada, se deberían definir estrategias y planes de actuaciones en caso de algún tipo de desastre, poseer algún tipo de sistema de detección de humo y fuego así como alarmas de incendio, poseer extintores o instalar puertas metálicas cortafuegos en las instalaciones donde se encuentren los sistemas de información.

Es muy importante en el acceso físico, al igual que en el acceso lógico, que los distintos accesos queden registrados para que el Responsable de Seguridad lo pueda supervisar después y realizar los informes oportunos.

- **Gestión de cuentas de servicios y contraseñas**

Tanto para la identificación y autenticación del personal como para el control de acceso a la información, es necesario muchas veces gestionar cuentas de servicios y contraseñas. Para ello se van a detallar una serie de pasos recomendados para una buena gestión (Colegio de Registradores de la propiedad y mercantiles de España, 2008).

En primer lugar, al Responsable del Fichero se le debe comunicar las necesidades de acceso a la información por parte de los usuarios para la elaboración de su trabajo. Y es éste quien aprueba o asigna los permisos. Además, deberá comunicar al Responsable de Seguridad esta información.
Estas solicitudes se corresponden con las altas y bajas del personal dentro de la empresa debido a un cambio en el puesto de trabajo o a las funciones desempeñadas o debido a un abandono del puesto de trabajo.

Una vez el Responsable de Seguridad reciba las solicitudes, comprobará las peticiones de las solicitudes con los requerimiento reales de cada puesto de trabajo. Si una solicitud se desestima se devolverá al Responsable del Fichero indicando la causa. En cambio, si la solicitud se aprueba se procederá a gestionarse.

Si se gestiona una solicitud, el Responsable del Sistema hará las modificaciones y cambios pertinentes en el sistema para que el usuario en cuestión tenga acceso o no a determinada información. En este punto se realizarán las altas, bajas o modificaciones de los permisos de acceso.

El Responsable del Sistema deberá seguidamente comunicar de forma segura los nuevos datos a los usuarios y también al Responsable de Seguridad. Este último, tal y como ya se ha indicado en puntos anteriores, deberá mantener actualizada la lista de usuarios con acceso autorizado al sistema de información. Esta actualización se debe materializar periódicamente en el Documento de Seguridad de la empresa.

- **Gestión de soportes**

Definimos soporte como *"objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos".*
Se considerarán como soportes todos los ordenadores de sobre mesa, ordenadores portátiles, teléfonos móviles, PDA's, discos duros USB, disco duros extraíbles, etc., siempre que sean utilizados para fines profesionales.

Como en estos soportes la mayoría de las empresas van a guardar información que contiene datos de carácter personales, hay que proteger estos soportes durante todo el proceso de su transporte o manipulación, y esto se realiza mediante un procedimiento de gestión de los soportes.

Medias de seguridad de nivel básico:

Todos los ficheros que contienen datos que requieren de un tratamiento de fichero de nivel básico deben contar con un tratamiento de gestión de los soportes.
Este procedimiento consiste básicamente en identificar los soportes, realizar un inventario de ellos, almacenarlos correctamente y restringir su acceso.

En primer lugar, el encargado de custodiar los soportes en la empresa deberá identificar los soportes que contengan datos de carácter personal indicando como mínimo en el etiquetado el código de soporte asignado, el tipo de información que contiene y la fecha de grabación o generación.

Además de la identificación, el Responsable de Seguridad debe mantener un inventario de todos los soportes. Este inventario deberá almacenar como mínimo los siguientes datos:

-Fichero o aplicación
-Tipo de soporte
-Ubicación del soporte
-Fecha de generación
-Fecha de destrucción/reutilización
-Responsable de custodia de soporte

Estos soportes deben almacenarse en un recinto seguro al cual sólo tengan acceso el personal autorizado. Estas autorizaciones deben reflejarse en el Documento de Seguridad.

Haciendo hincapié ahora en los ficheros y tratamientos no automatizados, recalcar tal y como se explicita en el artículo 108 del RDLOPD, que mientras la documentación con datos de carácter personal no esté archivada en los dispositivos establecidos, el responsable de custodiar los soportes deberá impedir en todo momento que una persona no autorizada tenga acceso a dicha información.

Por otra parte, para los ficheros no automatizados se establecerán unos criterios de archivo de modo que faciliten su consulta y localización para garantizar el ejercicio de los derechos ARCO.

Medias de seguridad de nivel medio:

Cuando se trate de ficheros cuyo tratamiento sea de nivel medio, además de aplicarle el tratamiento de gestión de soporte anterior, hay que registrar las entradas y salidas que se producen de los soportes.
En los registros de las entradas y salidas de los soportes se deberá mantener la siguiente información (artículo 97.1 y 97.2 del RDLOPD):

-Tipo de soporte
-Fecha y hora
-Emisor
-Número de documentos o soportes incluidos en el envío
-Tipo de información que contienen
-Forma de envío
-Persona responsable de la entrega, que debe estar debidamente autorizada
-Persona responsable de la recepción que debe estar debidamente autorizada

En el caso de que los soportes de salida vayan a ser desechados o reutilizados se deben ejecutar las medidas necesarias para que la información almacenada no se recuperable de ninguna forma.

A continuación se detallan varias medidas adecuadas para estos casos (Del Peso, 2004:282).
Si se trata de un equipo que contiene soportes como puede ser un servidor, un ordenador de sobremesa o un equipo portátil, se puede dar un nuevo formato y de esa forma se consigue un borrado profundo o se puede sobregrabar datos aleatorios en varias pasadas para que el contenido que había antes no sea accesible con ningún tipo de mecanismo sofisticado.
Por el contrario, si se trata de soportes extraíbles o soportes que no forman parte de un equipo y son magnéticos se pueden desmagnetizar, o también se podría incinerar, triturar o destruir.
Si son ópticos y no regrabables, entonces la mejor opción sería triturarlos o destruirlos.
Pero no siempre va a ser posible borrar o destruir los datos antes de destruir los soportes, así que si se contratan los servicios de una tercera empresa para destruir los soportes y estos todavía contienen datos de carácter personal, entonces se deberá exigir que firmen y cumplan unas cláusulas de confidencialidad para mantener a salvo los datos.

La autorización de la salida de los soportes físicos que contienen datos de carácter personal solamente podrá ser autorizada por el Responsable del Fichero o aquel en que hubiera delegado.

Medias de seguridad de nivel alto:

Y finalmente, para los ficheros que contienen datos de nivel alto, la entrada y salida de los soportes se realizará a través de mecanismos que puedan garantizar que esa información no sea inteligible y asegurar que esa información no pueda ser manipulada durante su transporte. Así que se identificarán o etiquetarán de forma confidencial. Dentro de cada soporte la información debe estar cifrada.

- **Acceso a datos a través de redes de comunicaciones**

Cada vez más empresas hacen uso de las nuevas tecnologías y han sustituido numerosos procedimientos de gestión en soporte papel, por gestiones que se pueden realizar a través de las telecomunicaciones. Estas gestiones implican que se transmiten por la red ficheros automatizados que contienen datos de carácter personal y que por ello hay que aplicar las medidas de seguridad correspondientes a esos ficheros. Los ejemplos más comunes de comunicaciones a través de redes son el correo electrónico así como todas las aplicaciones online que permiten transmitir datos en cualquier momento del día y desde cualquier computador.

Cuando deban implantarse medidas de seguridad de cualquiera de los tres niveles, la transmisión de datos de carácter personal, ya sea a través de redes públicas o de redes inalámbricas de comunicación electrónica, debe proteger y garantizar que la información transmitida no será legible ni manipulada por terceros.
Los accesos a través de las redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.
Además, si se trata de medidas de seguridad de nivel alto, la transmisión de estos datos se deberá cifrar o en su caso, utilizar cualquier otro mecanismo que pueda garantizar la protección total de la información.

Además, tal y como se indica en la página web de LOPDPLAN, los cuales son un grupo de empresas especializados en la informática y en la consultoría, se deberán establecer mecanismo de control sobre las posibles empresas externas autorizadas que se conecten a los sistemas informáticos de la empresa en cuestión y se deberá asimismo realizar controles periódicos de las actualizaciones y del correcto funcionamiento de los dispositivos de seguridad que se implanten en los puntos de acceso a los sistemas de información a través de las redes de telecomunicaciones externas.

- **Régimen de trabajo fuera de los locales de la ubicación del fichero**

En el caso de que sus trabajadores tengan que trabajar con ficheros fuera de los locales de la ubicación de estos, el Responsable del Tratamiento del fichero deberá tener autorización expresa del Responsable del Fichero, hacer constar este hecho en el Documento de Seguridad y garantizar en todo momento el nivel de seguridad que

corresponda. Todas las medidas de seguridad que se apliquen tendrán como finalidad evitar que terceros puedan acceder a los datos protegidos.

- **Ficheros temporales**

Muchas veces las empresas recurren a la creación de archivos temporales o copias de datos para ejecutar sus actividades, pero hay que tener en cuenta que estos archivos temporales han de ser creados exclusivamente para trabajos temporales o auxiliares y que deben de cumplir con una serie de medidas (Del Peso, 2004:275).

Los ficheros temporales se crearán cuando sean estrictamente necesarios y deberán ser autorizados por el Responsable del Fichero. Además, estos ficheros tendrán una finalidad específica y una duración prefijada, es decir, una período de vigencia máxima.

Estos ficheros pueden crearse o no automáticamente. Si un fichero en cuestión no es creado automáticamente por un sistema, entonces se le asignará un responsable el cual lo será tanto de su protección como de su uso.
Sin autorización del responsable no se podrán añadir ni modificar los campos de los ficheros temporales.

Y como estos ficheros contendrán datos de un cierto nivel, deberán cumplir con las medidas de seguridad de ese mismo nivel que dictamina la normativa y con las medidas que se incluyan en el Documento de Seguridad de la empresa.

Cuando su tiempo de vida establecido de antemano llegue a su fin, significará que el fichero temporal ya no cumple la finalidad originaria de modo que se borrará o se destruirá.

- **Copias de seguridad**

"Existe un solo motivo por el cual se pierde información: la falta de backups" (Cristian F. Borghello, 2002).

La copia de seguridad o copia de respaldo de un fichero (backup) es el método por el cual se copian los datos de dicho fichero. Esta copia permitirá restaurar, es decir, recuperar, los datos del fichero en el caso de que se produzca una pérdida de información.

Es imprescindible concienciar a todos los miembros de la empresa de la importancia de realizar copias de seguridad de los datos que manejan ya que muchas piensan que es una tarea molesta, tediosa y que incurre en una pérdida de tiempo significativa, pero realmente el simple hecho de realizar copias de seguridad pueden salvarnos en situaciones inesperadas. La pérdida de información puede ser debida a diversas causas como por ejemplo la eliminación involuntaria de datos por parte de algún empleado, la infección por algún virus o la pérdida o deterioro del soporte físico que almacene datos.

El beneficio de estar en posesión de una copia de seguridad es muchísimo mayor que los inconvenientes que repercute el hecho de realizarla.

Realmente, la realización de una copia de seguridad es fácil y hay múltiples posibilidades como realizar la copia en un CD o DVD, grabarla en una cinta, en discos duros extraíbles e incluso subir la información a hostings que cuenten con backups.

Medias de seguridad de nivel básico:

Para los ficheros automatizados las medidas de seguridad de nivel básico a aplicar según el Reglamento de Desarrollo de la LOPD son:

-Realización de una copia de respaldo semanal como mínimo. Se puede obviar la realización de la copia semanal en el caso de que no se haya producido ninguna actualización de los datos.
Se recomienda para una mayor seguridad, realizar una copia de seguridad diaria.

-Definir un procedimiento de generación de copias de respaldo y recuperación de datos que garantice en todo momento su reconstrucción en el estado en que se encontraba al tiempo de producirse la pérdida o destrucción.
La grabación podrá ser manual sólo en el caso de que exista documentación que lo permita y este hecho deberá constar en el Documento de Seguridad.

-Verificación semestral de dichos procedimientos por parte del Responsable del Fichero.

-Si se realizan 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 a no ser que se asegure el nivel de seguridad correspondiente y se haga constar en el Documento de Seguridad.

-En el caso de ficheros no automatizados no existe la obligación de realizar copias de respaldo.

Una de las medidas de seguridad de nivel básico es la definición de procedimiento de generación de copia de respaldo. Este procedimiento se debe elaborar por la empresa.

A continuación vamos a desarrollar un procedimiento base el cual cada empresa puede ampliar y modificar para satisfacer sus propias necesidades.

En primer lugar, la actividad a llevar a cabo sería preparar los soportes de grabación. El responsable de la realización de la copia de seguridad deberá comprobar la planificación y el etiquetado de los soportes que van a usarse en la copia. Si se el responsable detecta alguna anomalía la corregirá, ya sea cambiando el soporte por otro o etiquetando correctamente los soportes defectuosos.

Seguidamente, una vez la preparación de los soportes sea la adecuada, se procederá a la ejecución de la copia de seguridad. Esta ejecución podrá ser manual o automática y se recomienda fijar una periodicidad de ejecución y una hora concreta para su realización. Como ya se ha dicho, se recomienda la realización de copias de seguridad diarias.

Cuando se haya concluido la copia, el responsable designado deberá comprobar el resultado de esta. Si no ha habido errores se registrará el resultado mediante alguna herramienta y se almacenará el soporte en su lugar correspondiente. Si por el contrario, hubiera habido algún error en la copia, se registrará la incidencia y se resolverá.
Cada seis meses el Responsable del Fichero deberá verificar la copia de respaldo, restaurando la copia en un servidor de prueba para poder verificar el resultado de la misma.

Medias de seguridad de nivel alto:

En el caso de los ficheros automatizados de nivel alto, las copias de seguridad y procedimientos de recuperación se deberán almacenar en lugares diferentes del que se encuentren los equipos.

El hecho de que se deban guardar en un lugar físico diferente es para evitar que la información se encuentre sometida a las mismas contingencias que puede sufrir el lugar de almacenamiento habitual en el caso de que se produjera un accidente o desastre como por ejemplo una inundación o un incendio.

Si se diera el caso en que no fuera posible almacenar las copias de respaldo en lugares diferentes, entonces se deben adoptar medidas complementarias que reduzcan el riesgo de algún accidente o desastre, como por ejemplo implantando sistemas antiincendio.

- **Restauración de copias de seguridad**

La restauración de de copias de seguridad garantizan la reconstrucción de los datos de un ficheros al estado en el que se encontraba cuando se produjo el fallo.

Al igual que en la generación de copias de seguridad se establecía un procedimientos, en las restauración de las copias de seguridad también.

Cuando sea necesario realizar una restauración de una copia de seguridad, se deberá comunicar al Responsable de Seguridad la necesidad de restaurar los datos y este se encargará de registrar este hecho como una incidencia de seguridad e indicará el motivo que lleva a la restauración.

Si los datos de los ficheros que se van a restaurar son de nivel medio o alto, se necesitará la autorización por escrito del Responsable del Fichero.
La restauración se deberá realizar a través del procedimiento que la empresa haya definido. En el caso de que su empresa trabaje con aplicaciones externas de

recuperación, se deberá solicitar al proveedor el cumplimiento del procedimiento de recuperación definido por la empresa.

Una vez realizada la restauración, el Responsable de Seguridad deberá registrar en la incidencia anteriormente registrada los efectos derivados de la restauración y la resolución de la misma.
Si los datos restaurados son de nivel medio o alto, además se deberá detallar información como la persona que ha ejecutado el procedimiento de recuperación así como los datos restaurados.

- **Gestión de incidencias**

Con el término incidencia hacemos referencia a *"cualquier anomalía que afecte o pueda afectar a la confidencialidad, integridad o disponibilidad de los datos de carácter personal"* y a cualquier incumplimiento, que se produzca en nuestra empresa, de la normativa desarrollado en el Documento de Seguridad elaborado por la misma.

Medias de seguridad de nivel básico:

Todos los ficheros de los distintos niveles estarán obligados a mantener un sistema de notificación y registro de las incidencias.

En el procedimiento de la notificación se deberá especificar quién tiene que notificar la incidencia, a quién se lo comunicará y de qué modo. En empresas pequeñas al haber pocos usuarios, cualquier usuario que tenga conocimiento de una incidencia que implique un riesgo para la seguridad de los datos de carácter personal, debe comunicársela al Responsable del Fichero o a quién se le haya atribuido esta actividad.
El Responsable del Fichero debería sancionar a aquel usuario que conozca la existencia de una anomalía y no lo notifique.

El Responsable de Seguridad llevará a cabo el registro de las incidencias, preferentemente en soporte electrónico, y tendrá que registrar como mínimo los siguientes datos (art. 90 del RDLOPD):

-Nombre del fichero o nombre del sistema
-Tipo y descripción de la incidencia: acceso indebido, pérdida de datos, copia no autorizada, corrupción de datos, etc.
-Momento en que se ha producido o detectado
- Nombre de la persona que realiza la notificación
-Nombre de la persona a quien se comunica
-Efectos que se hubieran derivado de la misma
-Medidas correctoras aplicadas
-Sistema informático utilizado, en caso de gestión automatizada.

Una vez las incidencias hayan sido notificadas y registradas, el Responsable de Seguridad debe proceder a la resolución de la misma mediante medidas correctoras.

Además, se recomienda que periódicamente el Responsable de Seguridad revise el registro de incidencias y las medidas aplicadas para llevar a cabo un seguimiento de funcionalidad.

Medias de seguridad de nivel medio y alto

Los procedimientos de notificación, registro y gestión de las incidencias se disponen para ficheros de seguridad de nivel bajo, medio y nivel alto. Adicionalmente los ficheros de nivel medio y alto deben ejecutar un procedimiento de recuperación de datos en el caso de que para la resolución de una incidencia sea necesaria la restauración de los datos de una copia de seguridad de ficheros de datos de carácter personal.

Entonces, al registrar una incidencia se deben incluir los siguientes datos:

-Proceso de recuperación de datos utilizado
-Nombre de la persona que ejecuta el proceso
-Datos restaurados
-Datos que han sido corregidos de forma manual
-Autorización por escrito del Responsable del Fichero para reparar la incidencia

- **Auditoría**

Todas las empresas que estén en posesión de datos de carácter personal de nivel medio o alto deben realizar una auditoría interna o externa, al menos cada dos años, la cual corrobore el correcto funcionamiento y la adecuación del las medidas que se reflejan en el Documento de Seguridad.

En la auditoria interna se requiere la participación de personal interno experto en la materia de la empresa. En muchas empresas esta participación se plasma mediante un departamento de auditoría interna.
En la auditoría externa, se requiera la contratación de los servicios de un auditor externo con conocimientos en materia de seguridad de datos de carácter personal.

Si se realizan modificaciones relevantes en los sistemas de información, se puede elaborar una auditoría con carácter extraordinaria con el fin de verificar la adaptación, adecuación y eficacia de estas modificaciones.

El informe de auditoría elaborado por el auditor debe reflejar las deficiencias encontradas y proponer medidas correctoras para paliarlas. También debe de incluirse en el informe los datos, hechos y observaciones en que se basen sus argumentos (art. 96 del RDLOPD).

Estos informes de auditoría deben ser analizados por el Responsable de Seguridad, el cual comunicará las medidas correctoras necesarias al Responsable del Fichero para que este último las adopte.

Es muy importante la realización bianual de las auditorías ya que estos informes estarán a disposición de la Agencia Española de Protección de Datos.

En la guía “Guía para empresas: cómo adaptarse a la normativa sobre protección de datos” creada por INTECO, se refleja un ejemplo de procedimiento a seguir en una auditoría que puede ser útil para los que se estén introduciendo en la adaptación a la LOPD:

1. Realizar un inventario de ficheros

2. Para cada uno de los ficheros realizar las siguientes actividades:
   -Revisar el Documento de Seguridad
   -Revisar el acceso lógico a los datos de carácter personal de los ficheros automatizados
   -Revisar el acceso físico a los datos de carácter personal tanto de los ficheros automatizados como de los no automatizados
   -Revisar las políticas de copias de respaldo y gestión de soportes
   -Revisar el registro de incidencias

3. Para cada uno de los ficheros de nivel medio, realizar lo siguiente:
   -Revisar las anteriores auditorías
   -Revisar las pruebas con datos reales

4. Para cada uno de los fichero de nivel alto, realizar lo siguiente:
   -Revisar los registros de accesos
   -Revisar las telecomunicaciones

- **Pruebas con datos reales**

Puede que en su empresa todavía no haya instalado un sistema de información o una aplicación informática que trabaje con ficheros de carácter personal, en ese caso, si desea instalar un sistema nuevo o, por otra parte, modificar el que tuviera, debe tener en cuenta, que si los ficheros contienen datos de carácter personal de nivel medio, entonces no se podrán realizar pruebas previas a la instalación con datos reales, a no ser que se asegure el nivel de seguridad correspondiente al fichero tratado.

Para realizar la realización previa de pruebas se debe seguir un procedimiento que cumpla una serie de medidas de seguridad. A continuación se explicita un procedimiento de puede servir de modelo para las empresas:

En primer ligar, la persona encargado de realizar estas pruebas previas debe enviar una solicitud de autorización para el traslado o transferencia de los datos al Responsable del Fichero. Éste será quien evaluará y autorizará si lo considera oportuno, el envío de los datos al solicitante.

Una vez se haya obtenido la autorización se transmitirán los datos y se guardarán en un lugar con acceso controlado.
Tal y como anteriormente ya se ha explicado, esta transmisión, en el caso de tratarse de datos de nivel alto, se debe cifrar y garantizar que los datos no sean inteligibles ni sean manipulados.

Los datos transmitidos y almacenados pueden entonces ser tratados y manipulados por el encargado de realizar la prueba.
Si fuera necesario, en el tratamiento se puede hacer uso de ficheros temporales y/o copias de seguridad, siempre y cuando cumplan el nivel de seguridad que les corresponde por albergar datos de un cierto nivel.

Por último y para finalizar el procedimiento, el encargado de la realización de las pruebas previas, debe borrar los datos que se le habían transmitido para el tratamiento, así como los ficheros temporales y/o copias de seguridad que hubiera creado.

- **Controles periódicos**

La empresa elabora el Documento de Seguridad con sus respectivas normas de seguridad las cuales deben ser respetadas y cumplidas por todos los miembros de la empresa, pero para verificar y velar por el correcto cumplimiento de estas, se deberán realizar controles periódicos.

Se recomienda que para los ficheros de datos de **nivel alto**, el Responsable de Seguridad revise **mensualmente** los controles de acceso a los ficheros y que realiza un informe de las revisiones realizadas y los problemas detectados.

En cambio, los ficheros que contienen datos de **nivel medio** deberían controlares de **trimestralmente**. En este caso el Responsable de Seguridad debería:

-Comprobar que realmente la lista de usuarios que acceden a un determinado fichero corresponde a la lista de usuarios autorizados para acceder a dicho fichero.

-Verificar el cumplimiento de los previsto en los procedimientos de gestión de los soportes, en relación a las entras y salidas de datos, ya sea por red o en soporte magnético.

-Revisar, junto con el Responsable del Fichero, del Registro de Incidencias.

En cuanto a las **copias de seguridad** realizadas, las cuales permiten la recuperación de datos, deben ser controladas **semestralmente** por el Responsable del Seguridad

- **Revisión del Documento de Seguridad**

Es importantísimo que el Documento de Seguridad esté siempre totalmente actualizado, por ello debe ser revisado siempre que hayan cambios relevantes en el sistema de información o en su organización.

Puede que la legislación en materia de seguridad de los datos de carácter personal se vea modificada debido a los constantes debates políticos, de modo que el

Documento de Seguridad deberá adaptarse rápidamente a las nuevas exigencias en dicha materia.

Además, el Responsable de Seguridad puede en todo momento proponer una serie de cambios en el Documento que permitan mejorar la seguridad de los sistemas. En caso de que esto se produzca, el Responsable del Fichero deberá evaluar y aprobar estos cambios e informar de estos cambios a todos los miembros de la empresa que puedan verse afectados por estas modificaciones.

TRATAMIENTO DE DATOS EN EL ÁMBITO DE INTERNET:

- **Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)**

Como se ha ido repitiendo a lo largo de esta guía, la información que posee una empresa es el activo de mayor valor, y esta información, debido a las innovaciones y a los avances en las tecnologías, se almacena mayoritariamente en equipos informáticos. Además, la mayoría de empresas ya prestan sus servicios a través de la Internet, de ahí el nacimiento del comercio electrónico. Las empresas han adoptado las redes de comunicaciones e Internet como medio de transmisión e intercambio de información, lo cual ha repercutido en grandes ventajas para las distintas empresas y sus clientes, pero el uso de las nuevas tecnologías también ha generado ciertas incertidumbres, las cuales han sido aclaradas en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, que llamaremos LSSI. Esta ley se corresponde con la Ley 34/2002, del 11 de julio de 2002.

Esta Ley tiene como objeto la regulación y control de Internet con el fin de asegurar una completa seguridad electrónica así como garantizar los derechos y los deberes de los usuarios y de las empresas prestadoras de los servicios y en esta guía la vamos a tratar muy por encima ya que no es el objeto de la guía.

La LSSI contiene siete Títulos:

Título I	Disposiciones Generales
Título II	Prestación de Servicios de la Sociedad de la Información
Título III	Comunicaciones Comerciales por vía electrónica
Título IV	Contratación por vía electrónica
Título V	Solución Judicial y Extrajudicial de Conflictos
Título VI	Información y Control
Título VII	Infracciones y Sanciones

Vamos a definir en primer lugar el término Servicio de la Sociedad de la Información, que según la Confederación de Empresarios de Andalucía, se trata de *"todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. También comprende los servicios no remunerados por sus destinatarios, en la medida en que constituyen una actividad económica para el prestador de servicios."*

Esto último significa que dicha Ley sólo se aplica al comercio electrónico y a otros servicios de Internet cuando sean parte de una actividad económica.
Ejemplo de estos servicios de la sociedad de la información son:

-La contratación de bienes o servicios por vía electrónica
-La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales
-La gestión de compras en la red
-El envío de comunicaciones comerciales
-El suministro de información por vía telemática

El Ministerio de Industria, Turismo y Comercio de España redactó un folleto informativo llamado "LSSI. La Ley de Internet fácil". En dicho folleto el lector puede encontrar información más extensa sobre la LSSI.
A continuación se destacan los aspectos más relevantes de dicho folleto. Aspectos que dan a las empresas una visión global de sus obligaciones ante la aplicación del comercio electrónico, ante hacer publicidad por vía electrónica y ante la prestación de servicios de intermediación de información.

En el caso de que su empresa realice **comercio electrónico**, en su página web deberá aparecer la siguiente información (art. 10 LSSI):

-Denominación social, NIF, domicilio y dirección de correo electrónico, teléfono o fax
-Datos de inscripción registral
-Códigos de conducta a que esté adherida
-Precios de los productos o servicios que ofrecen, indicando los impuestos y gastos de envío
-Y en caso de ser necesario, datos relativos a la autorización administrativa necesaria para el ejercicio de la actividad; datos de colegiación y título académico de profesionales que ejerzan una actividad regulada; e información adicional cuando al servicio se acceda mediante un número de teléfono de tarificación adicional

Además, en este folleto se recalca que si una empresa determinada va a realizar contratos on-line, deberá añadir en su web también (art. 27 LSSI):

-Trámites que deben seguirse para contratar on-line
-Informar si el documento electrónico del contrato va a ser archivado y accesible
-Medios técnicos para identificar y corregir errores en la introducción de datos
-Lengua o lenguas en que se podrá formalizar el contrato
-Condiciones generales a que se sujete el contrato

Si su empresa hace **publicidad por vía electrónica** (art. 19-22 LSSI), entonces deberá identificarse claramente, deberá informar sobre el carácter publicitario del mensaje, así como indicar si se trata de ofertas, concursos u otros métodos promocionales y las condiciones de participación.

Si además su empresa envía mensajes SMS a través del correo electrónico deberá previamente haber obtenido la autorización expresa del destinatario, identificar el mensaje con la palabra "publicidad" o "publi" y permitir en cualquier momento que el usuario pueda darse de baja en ese servicio.

Hay algunas empresas que no se dedican al comercio electrónico propiamente dicho, sino que realizan **servicios de intermediación de la sociedad de la información**.
Un servicio de intermediación *"es en el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información"* (Confederación de Empresario de Andalucía).
Ejemplos de estos servicios son la transmisión de datos por redes de telecomunicaciones, la provisión de servicios de acceso a Internet, el alojamiento en los

propios servidores de datos, provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet, etc.

En este caso, las obligaciones de los prestadores de estos servicios son:

-Colaborar con los órganos públicos para le ejecución de resoluciones que no puedan cumplirse sin su ayuda

-Informar a los clientes sobre técnicas de seguridad como los anti-virus, anti-programas espía o filtros de correo; sobre las herramientas que existen para el filtrado y restricción de acceso a determinados servicios y contenidos; sobre las responsabilidades que tienen los usuarios en caso de hacer uso de Internet para fines ilícitos.

Para concluir este apartado se van a citar las tres actividades delictivas más comunes que afectan a la protección de datos y al comercio electrónico.
Debido a estas actividades y a otras muchas, la LSSI fue creada.

El *Phising* consiste en suplantar la identidad de una empresa a través del envío de comunicaciones electrónicas. Mediante esta actividad es fácil obtener información sobre los clientes de la empresa suplantada.

A través del *Spyware,* el cual es un programa de ordenador, se puede obtener datos de un determinado usuario que esté navegando por Internet. Estos datos pueden ser las direcciones IP, los números de tarjetas de créditos o las contraseñas.

Y la actividad más conocida es el *Spam* el cual consiste en el envío masivo de mensajes a correos electrónicos y a teléfono móviles. Todo usuario afectado por el *Spam* puede presentar una demanda a la AEPD porque la Agencia ha asumido esta competencia.

CONCLUSIONES

Llegados a este punto, se pretende que el lector de esta guía sea capaz de entender la legislación de materia de protección de datos personales, así como de adecuar su comportamiento para el pleno cumplimiento de la Ley Orgánica de Protección de Datos. Para conseguirlo, el lector debe seguir el Documento de Seguridad que su empresa haya elaborado.

Como ya hemos visto, hay multitud de razones por las cuales debemos adaptarnos a la LOPD y la más importante es la de cumplir con la normativa vigente y de este modo evitar sanciones, las cuales oscilan desde 600 euros a 600.000 euros. Por tanto, el no cumplimiento de la LOPD, puede incurrir en una gran pérdida económica para la empresa.

Además, debemos adaptarnos a la LOPD porque hoy en día la información está considerada como el activo de mayor valor de toda empresa. De modo que la empresa debe preocuparse por capacitar a todo su personal en materia de protección de datos para evitar que éstos cometan errores, negligencias o infracciones, las cuales pueden provocar pérdidas de información como por ejemplo datos de clientes.

Por otra parte, una empresa que cumpla con la LOPD siempre poseerá una buena imagen de cara a la sociedad, y esto le proporcionará notoriedad y generará confianza entre sus clientes. Una empresa siempre debe garantizar y asegurar la protección de los datos de carácter personal de sus clientes ya sea en los tratamientos de los datos, en las cesiones y demás operaciones que se realicen.

Hay que tener en cuenta que esta guía ha sido finalizada en abril de 2010, de modo que el lector deberá estar atento a los cambios y modificaciones que se puedan realizar en la normativa de protección de datos.

BIBLIOGRAFÍA:

Agencia Española de Protección de Datos (2009). www.agpd.es, 14/04/2009

AEPD (2008). "Guía de Seguridad de Datos". AEPD.

AEPD – Agencia de Protección de Datos (2008). "FAQs 1ª sesión anual abierta de la Agencia Española de Protección de Datos", Agustín Puente Escobar.

Bernal Montañés, Rafael; Coltell Simón, Óscar; (1996). "Auditoría de los Sistemas de Infomación", Servicio de Publicaciones UPV, Valencia.

BOE (2009). www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf, 26/03/2009

Borghello, Cristian (2002). www.segu-info.com.ar Buenos Aires, Argentina. 9/03/2010

Colegio de Registradores de la propiedad y mercantiles de España (2008). "Guía rápida Derechos ARCO". Registradores de España. Madrid.

Colegio de Registradores de la propiedad y mercantiles de España (2008). "Guía rápida sobre Responsabilidad y Roles". Registradores de España. Madrid.

Confederación de Empresarios de Andalucía (2009). www.cea.es/portalcea/proyectos/lopd/, 07/04/2010

Derecho.com & Jurisweb.com (1997). "Diccionario". www.derecho.com, 22/11/2009

European Data Protection Supervisor (2007). "Taller sobre la Aplicación de las leyes nacionales de Protección de datos". Bruselas

Extrenet (2009). "Normas y seguridad". www.extrenet.info/LOPD_SSI.pdf, 14/04/2009

HispaNetwork Publicidad y Servicios, S.L (2009). www.glosario.net, 14/08/2009

Instituto Nacional de Tecnologías de la Comunicación (2009). "Guía para empresas: cómo adaptarse a la normativa sobre protección de datos." INTECO

Leggio Contenidos y Aplicaciones Informáticas, S.L. (2009) www.noticias.juridicas.com, Zaragoza. 10/04/2010

LOPDPLAN (2001). www.lopdplan.com/LOPD.aspx, 28/02/2010

Microsoft (2009). www.microsoft.com/spain/empresas/guias/lopd/home.mspx, 14/04/2009

Ministerio de Industria, Turismo y Comercio (2009). "LSSI. La Ley de Internet fácil". www.mityc.es/dgdsi/lssi/Paginas/Index.aspx, 07/04/2010

Peso Navarro, Emilio del (2000). "Ley de Protección de Datos. La nueva LORTAD". Editorial Díaz de Santos, Madrid.

Peso Navarro, Emilio del; Ramos González; Miguel Ángel; Peso Ruiz, Mar (2004). “El Documento de Seguridad: Análisis técnico y jurídico. Modelo”. Ediciones Díaz de Santos.

PricewaterhouseCoopers Jurídico y Fiscal (2006). “Datos en Papel. Tratamiento de datos personales e información confidencial en soporte papel en la empresa española”. PricewaterhouseCoopers.

Protección Legal (2005). “Los códigos tipo en la LOPD”. www.proteccionlegal.com/proteccion-de-datos/articulos/86-los-codigos-tipo.html, 30/11/2009

Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.

Ribas, Xavier. Aspectos jurídicos de las tecnologías de la información (2006). http://xribas.typepad.com/xavier_ribas, 22/11/2009

Ribas, Xavier. El Reglamento de la LOPD. Impacto en las empresas (2007). http://xribas.typepad.com/xavier_ribas/lopd, 27/11/2009

Rueda López, Ana Isabel (2003) “Estudio del Sector Sanitario Privado frente a la Ley Orgánica de Protección de Datos”. Facultad de Informática, Universidad Politécnica de Valencia.

Tecnologiapyme (2009). www.tecnologiapyme.com/legislacion, 26/03/2009

GLOSARIO:

Para poder familiarizarse con la normativa, a continuación se muestra un glosario de términos útiles para el fácil entendimiento de la LOPD y de su Reglamento.
Estas definiciones han sido tomadas del artículo 3 de la LOPD y del artículo 5 del RDLOPD y ampliadas por diversas fuentes citadas en la bibliografía.

AFECTADO O INTERESADO: Persona física titular de los datos que sean objeto del tratamiento.

ÁREA DE TRABAJO: Área no pública de la empresa donde se ubican los puestos de trabajo y los sistemas de información.

ÁREA RESTRINGIDA: Área que contiene los armarios de comunicaciones, almacenamientos de copias de seguridad y la zona de archivo de la empresa. Debe contar con medidas de seguridad adicionales al Área de Trabajo para evitar el acceso de personal no autorizado.

CESIÓN O COMUNICACIÓN DE DATOS: Toda revelación de datos realizados a una persona distinta del interesado.

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.

DATOS DE CARÁCTER PERSONAL: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

DATO DISOCIADO: Aquél que no permite la identificación de un afectado o interesado.

DESTINATARIO O CESIONARIO: La persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

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 o del Responsable del Fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

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

FICHERO FÍSICO: Todo fichero creado mediante la organización de datos personales con independencia de la aplicación que los crea o los trata.

FICHERO LÓGICO: Fichero o conjunto de ficheros físicos, que contienen el mismo tipo de datos, y que son tratados para una misma finalidad o finalidades compatibles.

FICHERO NO AUTOMATIZADO: Todo conjunto organizado de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

FICHERO TEMPORAL: Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

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 profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número de teléfono, número de fax y dirección electrónica.
Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

NORMA: Requisito o regla de obligado cumplimiento que se debe seguir o al que se deben ajustar los sistemas y conductas, tareas, actividades, etc. de los usuarios de sistemas de información de la empresa.

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

PERSONAL: Persona que necesita de la utilización de los recursos de la empresa para desempeñar determinadas funciones.

PROCEDIMIENTO DE DISOCIACIÓN: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

RESPONSABLE DEL FICHERO: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento aunque no lo realice materialmente.

RESPONSABLE DEL TRATAMIENTO: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que adopta decisiones sobre las concretas actividades de un determinado tratamiento de datos.

RESPONSABLE DE SEGURIDAD: Persona o personas a las que el Responsable de Fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

SISTEMAS DE INFORMACIÓN: Conjunto de equipos, programas, ficheros automatizados y soportes empleados para el almacenamiento y tratamiento de los datos.

TERCERO: La persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del Responsable del Tratamiento, el Responsable del Fichero, del Encargado del Tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del Responsable del Tratamiento o del Encargado del Tratamiento.

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

USUARIO DE SISTEMAS DE INFORMACIÓN: Cualquier persona que pertenezca o colabore con una empresa y que requiera acceso a los recursos de la empresa como aplicaciones, sistemas operativos, bases de datos, cortafuegos y dispositivos de comunicaciones entre otros.

ANEXOS:

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

Anexo II Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Anexo III Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico