



## **Qué es la Protección de datos**

La protección de datos, es una **obligación legal**, pero también una necesidad de sentido común si queremos ser respetuosos con nuestros clientes, empleados y proveedores, al proteger sus datos y garantizar la seguridad y adecuación de los ficheros que los contienen

La normativa de protección de datos personales en el marco español va calando hondo en las empresas. A pesar de ello muchas de ellas la desconocen o sabiendo de ella no han adaptado sus procedimientos y sistemas de información.

## **La Ley Orgánica de Protección de Datos .**

**La LOPD** es la legislación que obligatoriamente deben de cumplir todas las organizaciones, asociaciones, comunidades de propietarios, empresas, autónomos, empresarios y profesionales., que en el desarrollo de sus actividades, usen o traten ficheros que contengan datos de carácter personal (*personas físicas identificadas o identificables* ) registrados en cualquier tipo de soporte (*manual ó informático*).

Podemos afirmar que todas las organizaciones, empresas y autónomos por pequeños que sean tiene ficheros con datos personales, y deben cumplir las obligaciones que regula la LOPD .....

“SINO QUIEREN ARRIESGARSE A LAS SANCIONES POR SU INCUMPLIMIENTO”.

## **La Protección de Datos de Carácter Personal**

Es una nueva Obligación para las Empresas y Profesionales y una materia que ha tomado importancia en los últimos años, fundamentalmente a raíz de la aprobación de la LO 15/1999 de Protección de Datos, convirtiéndose en una obligación a cumplir por las empresas si no quieren estar expuestas a duras sanciones por la Agencia Española de Protección de Datos.

Es ni mas ni menos que el Control sobre los ficheros y tratamientos de datos de carácter personal efectuados por las entidades públicas o privadas, para facilitarle el ejercicio de las acciones y actividades que le otorga la normativa a la Agencia de Protección de Datos sobre protección de datos de carácter personal como Autoridad de Control Española.

La LOPD afecta y es de aplicable obligación a todos los datos de carácter personal registrados en soporte físico (tanto ficheros informáticos como ficheros manuales), que los haga susceptibles de tratamiento, por lo tanto, cualquier persona que tenga ficheros con datos de carácter personal, ya sea una empresa, un arquitecto, un dentista, etc., han de cumplir con esta normativa.



La protección de datos que manejamos no es un trámite legal para sacarnos el dinero, sino una necesidad de sentido común en la gestión y uso de los datos de carácter personal, con el que acreditar que nuestros clientes y proveedores son importantes y por eso respetamos sus datos personales.

## **CAUSAS DE LA NO ADECUACION A LA LOPD**

### **1. Desconocimiento de la legislación.-**

Muchas empresas, sobre todo las pequeñas, desconocen realmente que existe una legislación en esta materia.

### **2. Desconocimiento de la importancia del concepto "intimidad" como derecho fundamental.-**

La Ley sitúa el concepto "intimidad" como un derecho fundamental. Desde la Constitución hasta una Ley Orgánica pasando por directivas europeas, queda claro que el propietario o *titular* de los datos personales es la misma persona y que cualquiera que los utilice tiene que tenerlo en claro.

### **3. Temas jurídicos y legales al mismo tiempo.-**

A la hora de ponernos manos a la obra en adecuar nuestra empresa nos encontramos que existen diversas medidas a implantar, tanto técnicas, como legales.

### **4 La Agencia Española de Protección de datos no llega al ciudadano.**

La AEPD ha centrado casi todos sus esfuerzos en hacer llegar sus tesis a las empresas y poco al ciudadano. Al menos sus frutos han sido así. Como usuarios, conocemos la OCU pero poco la Agencia Española, en cambio las empresas la conocen más, sobre todo por las posibles sanciones que podían incumplir, que en algunos casos pueden llegar hasta los 100 millones de las antiguas pesetas.

### **5 "Una obligación mas.."**

Coincide en el tiempo con una "avalancha" de nuevas leyes (medio ambiente, prevención de riesgos laborales, etc.). Y por ello muchas empresas aun teniendo claro que lo tienen que hacer la carpeta de protección de datos está en el montón de tareas de realizar..*"Para el año que viene"*

### **6 Acciones en terceros**

Algunas acciones a realizar se derivan en terceros: proveedores, clientes, grupos de empresas, administración, etc. No siempre en la empresa podemos ser conscientes del abanico de responsabilidades que se derivan, por ello.



Para la mayoría de empresas, que en España son de dimensión pequeña o mediana, la adecuación de sus ficheros y forma de trabajar con datos de carácter personal a los requerimientos legales supone un coste, sin que nadie les haya explicado las ventajas más allá de meterles miedo por las elevadas multas en caso de inspección por la Agencia de Protección de Datos.

La adecuación tiene implicaciones legales de tramitación, necesidades organizativas e informáticas en la protección de ficheros y necesidades de seguimiento de su cumplimiento . La dispersión de tarifas que se ofertan en el mercado es significativa y lo que se recibe a cambio suele ser lo mismo: unos documentos y unos manuales, que nadie lee y por lo tanto no se aplican.

Y no se leen ni aplican por un error de concepto: la protección de los datos que manejamos no es un mero trámite legal para sacarnos el dinero, sino una necesidad de sentido común en la gestión y uso de los datos de carácter personal, con el que acreditar que nuestros clientes, proveedores y empleados son importantes y por eso respetamos sus datos personales. Aquí entra lo que sería otro coste para las empresas: vigilar que la protección de datos se cumple día a día.

Tanto unas empresas, las que han registrado sus ficheros de datos personales, como las que no lo han realizado, habrían de aplicar el sentido común en la captación, gestión y uso de los datos de carácter personal además de cumplir con los trámites de registro de ficheros en la AGPD.

Los datos de carácter personal se piden y se obtienen (si nos los dan) para una finalidad en concreto. El uso para otras finalidades o por otras persona, no demuestra precisamente mucho respeto para con nuestros clientes o empleados, razón más que de sobra para no comprometer nuestra profesionalidad.

**Por sentido común:  
si tengo permiso los uso,  
si no lo tengo no los uso**



## **NIVELES DE SEGURIDAD**

Se definen tres Niveles de Seguridad, BÁSICO, MEDIO y ALTO, englobando cada uno al anterior como si se tratara de un sistema de capas concéntricas donde la más alta contiene a la inferior.

**BÁSICO**.- Se aplica a todos los ficheros que contienen datos de carácter personal.

**MEDIO**.- Contiene además información sobre cuestiones administrativas, penales, hacienda pública, servicios financieros o cuando varios datos en su conjunto permitan obtener el perfil de un individuo o solvencia de una empresa.

**ALTO**.- Contiene datos sobre ideología, religión, orientación sexual o política, salud, datos policiales

## **MEDIDAS DE SEGURIDAD POR NIVELES**

### **NIVEL BÁSICO :**

- Elaboración del Documento de Seguridad
- Plan de incidencias y registro de las mismas
- Identificación y autenticación de los usuarios
- Control de accesos Y Gestión de Soportes
- Protocolos de copias de seguridad

### **NIVEL MEDIO :**

- Documento de seguridad (más requisitos que el anterior)
- Responsable de Seguridad (obligatorio)
- Auditorias y Plan de incidencias y registro de las mismas
- Identificación y autenticación de usuarios
- Diseño de sistemas de control y Gestión de soportes
- Protocolo copias de seguridad
- Pruebas con datos ficticios o con altas medidas de seguridad

### **NIVEL ALTO .**

- Documento de seguridad (más requisitos que el anterior)
- Responsable de Seguridad (obligatorio)
- Auditorias (externas o internas)
- Plan de incidencias y registro de las mismas
- Identificación y autenticación de usuarios
- Diseño de sistemas de control
- Distribución de soportes y encriptación para transporte de datos
- Copias de seguridad en lugares físicos diferentes
- Encriptación de datos a través de redes



## INFRACCIONES

LEVES .- No solicitar la inscripción de 601,01 a 60.101,21 €

GRAVES .- No inscribirse después de ser requerido DE 60.000 hasta los 300.506,05 €

MUY GRAVES .- hasta 601.012,10 €

## OBLIGACIONES BÁSICAS IMPUESTAS POR LA LOPD

Las obligaciones básicas impuestas por la LOPD se pueden resumir en:  
LEGALIZAR, LEGITIMAR Y PROTEGER

**1. LEGALIZAR.** Todos los ficheros (TODOS) de datos de carácter personal deberán estar inscritos y legalizados ante la Agencia Española de Protección de Datos.

**2. LEGITIMAR.** Todos los datos de carácter personal recogidos por la empresa, deben contar con el consentimiento del afectado, así como cumplir una serie de principios básicos como son:

**A. Principio del consentimiento del afectado.**

**B. Principio de información**

**C. Principio de calidad de los datos**

**A. Por principio del consentimiento,** entiende la Ley que es la manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de los datos personales que le son recabados.

Cuando una empresa decide recabar datos de carácter personal debe, para poder utilizarlos, recabar el consentimiento de la persona que los cede. Ello supone que el consentimiento del afectado deberá ser precedido por una declaración del Responsable del Fichero (la empresa que los recaba) en la que se indiquen, de forma clara y fácilmente comprensible, los datos que van a ser objeto de tratamiento y las finalidades a que van a ser destinados, para que los interesados indiquen, sin ningún género de dudas, su conformidad con su tratamiento.

En cuanto a las excepciones sobre que el consentimiento sea expreso e inequívoco, encontramos las siguientes:

1º.- No es necesario recabar el consentimiento del afectado cuando los datos de carácter personal se recojan para el ejercicio propio de las Administraciones Públicas.

2º.- Tampoco es necesario el consentimiento cuando los datos se refieran a las partes de un contrato o precontrato en una relación laboral o administrativa y sean necesarios para el cumplimiento o el mantenimiento de las obligaciones nacidas del mismo.

3º.- No será necesario el consentimiento del afectado si los datos son recabados de fuentes accesibles al público. Pero, se informará al interesado que sus datos proceden de estas fuentes.



**B. El principio del deber de información**, es la obligación que tienen las empresas de informarnos, de forma previa a la recogida, de modo expreso, inequívoco y preciso de lo siguiente:

1º.- De la existencia de un "fichero" al que serán incorporados los datos que nos solicitan.

2º.- Del carácter obligatorio o facultativo de consignar determinados datos.

3º.- De las consecuencias de la obtención de los datos.

4º.- De la posibilidad del ejercicio de los derechos de acceso, rectificación, cancelación u oposición al tratamiento de los datos.

5º.- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

**C. El principio de calidad de los datos**, hace referencia a que los datos son recogidos para una concreta finalidad, y no podrán ser destinados por el Responsable del Fichero a otras finalidades. La finalidad también nos permite reconocer qué fichero es al que deben dirigirse los interesados para ejercitar los derechos reconocidos por la Ley: los derechos de acceso, modificación, oposición y cancelación.

Además, hay que tener en cuenta las precauciones a adoptar en el caso de que los datos de carácter personal vayan a ser cedidos a otras empresas, o bien cuando el tratamiento de estos datos se va a efectuar por cuenta de tercero, ya que deberán realizarse contratos específicos.

**3. PROTEGER.** La LOPD y el Reglamento de Medidas de Seguridad (RD 994/1999), establecen la obligación de establecer una serie de medidas de carácter técnico y organizativo que garanticen la seguridad de los datos. Entre estas medidas se incluye la elaboración de un Documento de Seguridad en el que se detallarán los datos almacenados, las medidas de seguridad adoptadas, así como las personas que tienen acceso a esos datos.

*“El cumplimiento de cada una de estas obligaciones tan sólo exige un pequeño esfuerzo de las empresas y profesionales, que junto al asesoramiento adecuado, evitará disgustos y la imposición de duras sanciones económicas.”*

## **La Información Corporativa Confidencial**

Es uno de los principales activos de las empresas y como tal, debe estar protegida con medios técnicos y legales de accesos no autorizados.

El establecimiento de Pactos de Confidencialidad con trabajadores y terceras empresas nos permitirá proteger la Información Corporativa Confidencial, estableciendo expresamente las obligaciones y límites que se han de tener en cuenta en su tratamiento.

El incumplimiento de los Pactos de Confidencialidad puede suponer el inicio de acciones legales, y la reclamación de indemnizaciones por daños y perjuicios.

### **1.- ¿Qué entendemos por Información Confidencial?**



“Confidencial” es lo que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas”. Así, el empresario tiene la libertad de calificar como Confidencial, cualquier documento o información, que a su juicio, influya directa o indirectamente en el desarrollo del negocio.

Esta Información Confidencial ha de gozar de una protección especial, tendente a evitar su filtración, divulgación o difusión a terceros, acciones que pueden causar graves perjuicios a su empresa.

## **2.- Protección interna de la Información Confidencial de la empresa.**

Respecto a la Protección de la Información Confidencial dentro de la propia empresa hay que distinguir entre los trabajadores y el personal de alta dirección, que por razón de su puesto y funciones, accede o trata dicha Información.

En cuanto a los Trabajadores, se entiende que existe una obligación de confidencialidad y secreto intrínseca a la relación laboral, incluso cuando no exista una referencia expresa a la misma en el Contrato de Trabajo o no se hayan firmado Acuerdos de Confidencialidad específicos. Así, se entiende que el deber de confidencialidad y secreto se encuentra recogido por el Art. 5 Estatuto de los Trabajadores. A pesar de esto es recomendable incluir en los Contratos Laborales Pactos de Confidencialidad, que establezcan claramente las obligaciones de los trabajadores en este sentido informando a los trabajadores de las pautas a seguir en el tratamiento de la Información Confidencial, sus obligaciones y los límites establecidos, pudiendo, con esta medida, reducir algunas prácticas que se dan en el mundo empresarial (por ejemplo: llevarse las bases de datos o información confidencial o reservada, desarrollos de nuevos productos, etc... en el momento de abandonar el puesto laboral) o, en caso contrario, tener un documento que pueda servir como prueba en juicio en el que se manifiesta expresamente la obligación de confidencialidad y secreto, y el conocimiento del trabajador de tal obligación.

En cuanto al Personal de Alta Dirección, y dado que por razón de su cargo acceden a información especialmente sensible y/o confidencial, existe la obligación expresa de mantener la confidencialidad y secreto de las informaciones a las que tiene acceso por razón de su cargo, siendo práctica habitual el firmar Acuerdos específicos de confidencialidad junto con los Contratos de Trabajo, bien a través de una cláusula específica de confidencialidad en los Contratos, o bien incluyendo un Pacto o Acuerdo de Confidencialidad como Anexo al contrato principal de trabajo.

Además de la obligación de confidencialidad específica que tiene el personal de alta dirección de las empresas, hay que hacer referencia al pacto de no competencia, es decir, aquel por el que un personal de alta dirección no podrá celebrar contratos de trabajo con otras empresas, salvo autorización del empresario o pacto escrito en contrario (Art. 8 RD 1382/1985).

La empresa deberá tener establecidos medios técnicos u organizativos que permitan la protección de la información confidencial. Así es recomendable establecer las siguientes medidas de protección:



**-Limitar** el acceso a la información confidencial. Es decir, permitir el acceso a dicha información sólo al personal que por razón de su cargo o funciones es necesario que acceda a dicha información, no permitiendo tal acceso al resto del personal.

**-Establecer** medidas técnicas que permitan la visualización o tratamiento de información confidencial (por ejemplo: uso de contraseñas para el acceso a los documentos, criptografía, etc...).

**-Mantener/Almacenar** los documentos confidenciales en soporte papel, en armarios que se encuentren cerrados bajo llave o cajas fuertes, a las que sólo tengan acceso las personas autorizadas.

**-Realizar** de copias de seguridad que eviten la pérdida de información confidencial o sensible en caso de catástrofe, guardando una copia fuera de las instalaciones principales de la empresa.

Por último, y en relación a la protección de la información confidencial dentro del ámbito interno de la empresa, hay que señalar que en la prestación de determinados servicios se accede a información confidencial de terceros, existiendo de este modo, una obligación específica de confidencialidad con respecto a esa tercera empresa, obligación de confidencialidad que se extiende a los trabajadores que tratan dicha información, y que por tanto, debe quedar expresamente regulada a nivel interno, a fin de evitar posibles responsabilidades derivadas de la negligencia de algún trabajador de la empresa.

**3. Protección de la Información Confidencial** de la empresa cuando es tratada por terceros. Los contratos de **outsourcing**.

Cuando una empresa vaya a encargar la prestación de un determinado servicio, que implique el tratamiento o acceso a información confidencial por parte de terceras empresas, es recomendable incluir en el Contrato de Prestación de Servicios, una cláusula específica de confidencialidad, o bien, firmar directamente con cada una de las personas que accedan a dicha Información, Pactos o Acuerdos de Confidencialidad específicos.

Igualmente, y cuando la prestación del servicio implique el tratamiento de bases de datos titularidad de un tercero, es necesario tener en cuenta los aspectos recogidos en el artículo 12 de la LOPD, “Acceso a Datos por Cuenta de Terceros”, que ya fueron desarrollados en el artículo

#### **4.- Contenido básico de un Acuerdo o Pacto de Confidencialidad.**

-Establecer claramente qué se entiende por Información Confidencial. En este sentido, se puede establecer el deber de guardar secreto respecto de toda o determinada información tratada, siendo recomendable huir de referencias genéricas a la confidencialidad.

-Establecer claramente los medios, recursos o información que se pone a disposición del trabajador o tercera empresa, determinando la titularidad de la misma.

-Establecer específicamente la obligación de secreto y confidencialidad, el deber de actuar diligentemente en cuanto al tratamiento, conservación, almacenamiento, transporte, etc... Estableciendo que en todos los casos deberán



adoptarse los medios que aseguren y garanticen dicho secreto, y se evite su pérdida o el acceso a la misma de terceros no autorizados.

-Establecer la obligación de devolver la información confidencial a la que se ha tenido acceso en el momento que termine la relación contractual, estableciendo, igualmente, que a pesar de dicha terminación, la obligación de confidencialidad y secreto permanecerá vigente durante el plazo que sea establecido por las partes (la práctica habitual en este sentido, es establecer un plazo de 2 años después de finalizada la relación contractual).

-Es conveniente, igualmente, informar de las consecuencias que pueden derivarse del incumplimiento de dicha obligación de confidencialidad y secreto. Así puede establecerse que la sustracción o revelación de dicha información puede ser constitutivo de un ilícito de naturaleza penal (Art. 197 CP del descubrimiento y revelación de secretos), puede ser objeto de acciones disciplinarias (despido disciplinario en caso de que el incumplimiento venga por parte de un trabajador), reclamación de indemnizaciones por daños y perjuicios, etc...

-Por último, en los Acuerdos o Pactos de Confidencialidad pueden establecerse todas las especialidades, que por razón de la relación contractual que se establece, sean establecidas por las partes.

#### **5.- Límites de la Obligación de Confidencialidad y Secreto.**

Hay que señalar que la Obligación de Confidencialidad y Secreto queda limitada en aquellos casos en los que, por imperativo legal, la parte obligada sea requerida por un organismo jurisdiccional o administrativo para facilitar determinada información.

En estos casos, deberán ser atendidas aquellas órdenes en las que:

- La obligación de entrega venga determinada de manera concreta en la orden.
- Sea dictada por una administración o juzgado competente.
- Sea firme.

En estos casos, se informará a la otra parte de inmediato sobre el requerimiento recibido, siempre que no exista obligación de guardar secreto sobre el mismo  
Por mandato legal, administrativo o judicial.

#### **Ámbito de aplicación de la LOPD**

¿Qué datos/ficheros se regulan por la LOPD y cuáles no?. Una de las principales dudas que se encuentran los empresarios y profesionales con respecto a la LOPD es la determinación de qué Ficheros o Datos de Carácter Personal tratados se encuentran amparados por la normativa.

##### **A. Ámbito de Aplicación Material**

¿Qué datos se encuentran incluidos en la LOPD?. La LOPD establece su ámbito de aplicación en el artículo 2, al establecer que “la presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”



Así, para la determinación de qué concretos Ficheros o Datos de carácter personal entran dentro del ámbito de aplicación de la LOPD debemos tener en cuenta tres conceptos: “dato personal”, “fichero” y “tratamiento”.

**-“Dato de carácter personal”.**

Entendido como cualquier información concerniente a personas físicas, identificadas o identificables; es decir, toda información numérica, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Así, de cara a la ley, dato de carácter personal es cualquier elemento que permite determinar, de manera directa o indirecta, la identidad física, fisiológica, psíquica, económica, cultural o social de una persona física.

**-“Fichero”.**

Entendido como conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Es, por tanto, el soporte físico, sea automatizado o no, en el que se recoge y almacena, de manera organizada, el conjunto de datos que integra la información.

**-“Tratamiento”.**

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

Si bien entendemos que los ficheros de datos de carácter personal que se mantengan en soporte informático o telemático no presentan grandes dudas para su determinación, puesto que para su creación se exige, con carácter previo, la grabación, depuración y estructuración de una forma determinada, no sucede lo mismo para los ficheros en soporte papel (o ficheros no automatizados).

Para poder determinar cuando los datos registrados en soporte papel son susceptibles de tratamiento, y en consecuencia, se encuentren incluidos en el ámbito de aplicación de la LOPD, hay que atender a los siguientes requisitos:

-Que el tratamiento no automatizado se refiera a datos comprendidos en un Fichero en soporte papel.

-Y, que dichos datos se encuentren organizados estructurados u ordenados por criterios específicos. no considerándose, en consecuencia Fichero, la existencia de carpetas no estructuradas, aunque éstas contengan datos de carácter personal (por ejemplo: en una consulta médica las carpetas o fichas de pacientes ordenadas alfabéticamente por el nombre de los mismos, se consideraría un fichero susceptible de tratamiento, siéndole por tanto de aplicación la LOPD).

De este modo, la Ley concibe los Ficheros protegidos desde una perspectiva dinámica; es decir, no los entiende como un mero depósito de datos, sino, como una globalidad de procesos o aplicaciones que se llevan a cabo con los datos almacenados (por ejemplo: en la consulta médica en la que los datos de los pacientes están recogidos en fichas, las mismas no suponen un mero depósito de datos, sino que permiten al médico efectuar un análisis de las distintas visitas



que ha efectuado el paciente, revisar la historia clínica del paciente, y ofrecer un tratamiento o diagnóstico que se adapte a las circunstancias concretas de cada paciente).

**B. *Ámbito de Aplicación Temporal.***

**C.**

**¿Qué plazo existe para la adaptación de los Ficheros a la LOPD?**

Todos los ficheros de datos de carácter personal, automatizados o no, creados después de la entrada en vigor de la Ley deberán adecuarse a la normativa. Según la Disposición Final Tercera, la LOPD entró en vigor el 14 de Enero de 2000.

El principal problema reside en la adecuación de los ficheros de datos preexistentes a dicha fecha. La Ley vino a establecer un régimen transitorio para los mismos en su Disposición Adicional Primera:

- Para ficheros automatizados preexistentes al 14 de Enero de 2000, se establece que “los ficheros y tratamientos automatizados inscritos o no en el Registro de Protección de Datos deben adecuarse a la LOPD dentro del plazo de tres (3) años a contar desde su entrada en vigor...”. Este plazo adicional para la adecuación a la LOPD finalizó el pasado 14 de Enero de 2003.

- En relación a los Ficheros no automatizados preexistentes a la entrada en vigor de la LOPD –“su adecuación a la LOPD deberá cumplimentarse en el plazo de doce (12) años a contar desde el 24 de Octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados”. De este modo, los ficheros no automatizados preexistentes a la entrada en vigor de la LOPD no se encuentran incluidos en el ámbito de aplicación de la LOPD hasta el 24 de Octubre de 2007, pero si les son de aplicación las obligaciones descritas para el ejercicio de los derechos de los usuarios (derechos de acceso, rectificación, cancelación y oposición).

**C) Ficheros excluidos del ámbito de aplicación de la LOPD.**

El régimen de protección de los datos de carácter personal establecido por la LOPD no será de aplicación a:

-A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domesticas.

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

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

**D) Ficheros regulados por normas específicas.**

El artículo 2.3. De la LOPD establece que se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por la LOPD, los siguientes tratamientos de datos personales:

-Los ficheros regulados por la legislación de régimen electoral.



- Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
- Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las fuerzas armadas.
- Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes.
- Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación DE LA MATERIA.

**Inscripción notificación de ficheros en la agencia española de protección de datos.**

**Procedimiento,** Una vez han sido localizados y determinados los ficheros de datos de carácter personal se procederá a la Notificación de los mismos a la Agencia Española de Protección de Datos para su Inscripción.

**a) Objetivos de la Notificación / Inscripción de Ficheros.**

**1.- Para la Agencia Española de Protección de Datos:**

- Control sobre los ficheros y tratamientos de datos de carácter personal efectuados por las entidades públicas o privadas, para facilitarle el ejercicio de las acciones y actividades que le otorga la normativa sobre protección de datos de carácter personal como Autoridad de Control Española.
- Determinar el grado de adecuación de dichos tratamientos a la normativa sobre protección de datos de carácter personal, y requerir a los responsables de los ficheros la adopción de las medidas de seguridad y procedimientos que garanticen la protección de los datos contenidos en los ficheros.
- Conocer la existencia de Transferencias Internacionales de Datos que requieran de autorización del Director de la Agencia Española de Protección de Datos.
- Permitir el ejercicio de los derechos de consulta de los titulares de los datos incluidos en los ficheros.

**2.- Para las Entidades Privadas:**

- Evitar la imposición de sanciones. En concreto la falta de notificación e inscripción de ficheros es calificada como infracción leve o grave (dependiendo de la magnitud del incumplimiento), sancionadas con multas de entre 601 € y 300.506 €.

No obstante, hay que señalar que la notificación e inscripción de ficheros es meramente declarativa, no prejuzgando el cumplimiento del resto de la normativa de protección de datos de carácter personal.

- Buena imagen exterior.

El cumplimiento de la normativa sobre protección de datos de carácter personal nos creará una buena imagen de cara a nuestros clientes y



potenciales clientes, aportándoles seguridad y confianza con respecto a nuestra empresa.

Igualmente, el incumplimiento de esta normativa y la imposición de sanciones por su incumplimiento, generarán en nuestros clientes y potenciales clientes una imagen negativa, pues las personas son día a día más conscientes de la importancia de la protección de su intimidad mediante el tratamiento diligente de sus datos.

**-Facilita las labores de control interno de la empresa.**

Puesto que el cumplimiento de la normativa sobre protección de datos de carácter personal implica la adopción de medidas de seguridad de carácter técnico (que pueden ser aprovechadas para la protección del resto de información corporativa de la empresa), así como la implantación de procedimientos organizacionales, las labores de control interno se ven agilizadas y facilitadas.

**b) Principios que rigen la notificación e inscripción de Ficheros:**

1. El Responsable del Fichero deberá notificar a la Agencia Española de Protección de Datos, previamente a la realización de cualquier tratamiento, la creación de un Fichero de datos de carácter personal.
2. La notificación e inscripción del Fichero tiene efectos meramente declarativos, no prejuzga el cumplimiento del resto de las obligaciones establecidas por la normativa sobre protección de datos de carácter personal.
3. La notificación de Ficheros implica el compromiso de asegurar el cumplimiento de las exigencias legales en el tratamiento de datos de carácter personal declarado para su inscripción.
4. La notificación de Ficheros tiene como finalidad principal asegurar la publicidad de las características y finalidades de los tratamientos.
5. Deberá notificarse a la Agencia Española de Protección de Datos cualquier cambio que se produzca con respecto a la declaración inicial.

**Las medidas de seguridad en la protección de datos de carácter personal.**

Todas las empresas, independientemente de su tamaño, organización y volumen de negocio, son conscientes de la importancia de tener implantadas una serie de políticas de Seguridad tendentes a garantizar la continuidad de su negocio en el caso de que se produzcan incidencias, fallos, actuaciones malintencionadas por parte de terceros, pérdidas accidentales o desastres que afecten a los datos e informaciones que son almacenados y tratados, ya sea a través de sistemas informáticos como en otro tipo de soportes, como el papel.

Desde el punto de vista de la Ley Orgánica de Protección de Datos, las medidas de seguridad van destinadas a todas las organizaciones, empresas e



instituciones que almacenan y tratan datos de carácter personal en sus sistemas de información, siendo su finalidad principal proteger los datos de carácter personal tratados de posibles incidencias que puedan provocar su pérdida, alteración u acceso no autorizado (tanto interno como externo).

Es importante señalar que tanto la Ley Orgánica como el Real Decreto 994/1999 que desarrolla el Reglamento de Medidas de Seguridad ligan el concepto de seguridad de los datos a los conceptos de:

- a) Confidencialidad: entendido como el acceso autorizado a los datos.**
- b) Exactitud: la información no debe sufrir alteraciones no deseadas, en cuanto a su contenido.**
- c) Disponibilidad: sólo las personas autorizadas pueden tener acceso a la información.**

Así podemos observar que la normativa, fijada para ofrecer unos mínimos de seguridad en el tratamiento de los datos de carácter personal, busca el ofrecer unas directrices de seguridad informática que pueden ser adoptadas e implantadas en todas las empresas, independientemente de su tamaño y organización.

## **1.- El Reglamento de Medidas de Seguridad.**

El Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de Medidas de Seguridad para los Ficheros automatizados de Datos de Carácter Personal establece las medidas de carácter técnico y organizativo que deben ser adoptadas por todas las Empresas, Organizaciones, Asociaciones e Instituciones, tanto Públicas como Privadas, que almacenen, traten y accedan a ficheros de datos de carácter personal.

Es una norma de mínimos, que siempre estará en función de tres extremos:

- a) La tipología de los datos y el tratamiento concreto que se realiza de los mismos.**
- b) La dimensión y estructura de los sistemas de información.**
- c) El estado de la tecnología.**

La obligación de seguridad que regula el Art.9 de la Ley Orgánica, desarrollada por este Reglamento, es una obligación de medios; es decir, nos obliga a adoptar las medidas necesarias para proteger los datos, pero reconoce que ninguna empresa puede garantizar al 100% que, con la adopción de dichas medidas, no vayan a producirse o existir incidencias.

Por ello, siempre que el Responsable del Fichero pueda acreditar que estableció y siguió las medidas de seguridad exigibles en cada caso, evitará una posible sanción por parte de la Agencia Española de Protección de Datos.

El Reglamento tiene por objeto determinar las medidas técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información



que contenga datos personales con la finalidad de preservarlos frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas que deberán ser adoptadas e implantadas por el Responsable del Fichero, y en su caso por el Encargado del Tratamiento, en los Sistemas de Información, en los Locales donde se realiza el tratamiento y sobre las personas que acceden a dicha información, Y son:

a) Medidas Organizativas: aquellas medidas destinadas a establecer procedimientos, normas, reglas y estándares de seguridad, cuyos destinatarios son los usuarios que tratan los datos de los ficheros.

Estas medidas deben tender a garantizar la confidencialidad, integridad y seguridad de los datos almacenados en programas y sistemas informáticos, que se encuentran situados físicamente en un determinado local o centro.

b) Medidas Técnicas: medidas destinadas principalmente a la conservar la integridad de la información (su no alteración, pérdida o robo) y en menor medida a la confidencialidad de los datos personales. Se encuentran delimitadas en función del nivel de seguridad de los datos tratados: básico, medio y alto.

Los destinatarios de estas medidas son los sistemas de información, ficheros, locales, equipos y demás elementos materiales que tratan los datos.

b) **Ámbito de aplicación.**

Las medidas técnicas y organizativas establecidas por el Reglamento deben aplicarse sobre:

- Los ficheros automatizados, entendidos como todo conjunto organizado de datos de carácter personal, cualquiera que fuere su forma o modalidad de creación, almacenamiento, organización y acceso.

- Los centros de tratamiento, entendidos como los lugares habilitados donde se encuentran los ordenadores, equipos y servidores que almacenan la información.

- Los locales, entendidos como aquellos lugares donde se encuentran físicamente ubicados los equipos y el personal que trata datos.

- Los equipos: todo material en soporte físico que sirva para tratar y almacenar electrónicamente datos personales.

- Los sistemas y programas informáticos que tratan los datos de carácter personal.

- Las personas que acceden a los datos: personal laboral que, de acuerdo con sus funciones y obligaciones, interviene en cualquiera de las fases del tratamiento de los datos (recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación, consulta, etc...).

c) **Ámbito de Exclusión.**

Quedan excluidos de la adopción de dichas medidas de seguridad:

- Los ficheros en soporte papel cuya creación sea anterior a la entrada en vigor de la Ley Orgánica 15/1999.

- Los ficheros automatizados que no contengan datos personales.

- Los ficheros automatizados personales para el ejercicio de actividades personales y/o domésticas (como por ejemplo, la agenda telefónica o la libreta de direcciones de los programas de correo electrónico).



**En el siguiente cuadro se muestran las diferentes medidas aplicables a cada uno de los niveles:**

MEDIDAS DE SEGURIDAD	BÁSICO	MEDIO	ALTO
Documento de Seguridad			
Identificación y Autenticación:			
1.- Existencia de una lista actualizada de usuarios autorizados que tengan acceso autorizado al sistema de información (Art.11.1 y 12.3).	✓	✓	✓
2.- Procedimientos de identificación y autenticación informáticos:			
a) Contraseñas: procedimiento de creación, asignación, conservación y cambio periódico (Art.11.2 y 11.3).	✓	✓	✓
b) Identificación de usuario, de manera inequívoca y personalizada (Art.18.1).		✓	✓
c) Limitación de acceso incorrecto reiterado (Art.18.2).		✓	✓
Control de Acceso:			
1.- Los usuarios tendrán únicamente acceso a los datos/recursos de acuerdo a su puesto laboral y tareas definidas en el documento (Art.12.1).	✓	✓	✓
2.- Deberán implantarse mecanismos que eviten el acceso no autorizado a otros recursos: establecimiento de perfiles de usuario (Art.12.2).	✓	✓	✓
3.- Control de acceso físico a servidores y CPD (Art.19).		✓	✓
4.- De cada acceso se guardarán: identificación usuario, fecha y hora, fichero accedido, tipo de acceso y su autorización o denegación, guardando la información que permita identificar			✓



registro accedido (Art.24.2).			
5.- Los mecanismos de acceso estarán bajo el control directo del Responsable de Seguridad, sin que pueda permitirse la desactivación (Art.24.3).			✓
6.- Registro y conservación de accesos lógicos al fichero por un plazo no inferior a 2 años (Art.24.4).			✓
7.- Para accesos a través de redes de telecomunicaciones, deberán tener las mismas medidas que para accesos en modo local (Art.5).	✓	✓	✓
Funciones y obligaciones del personal:			
1.- Definición en el Documento de Seguridad de las funciones y obligaciones de grupos de usuarios y/o perfiles (Art.9.1).	✓	✓	✓
2.- Conocimiento por parte del personal de las normas y medidas de seguridad que les son aplicables (Art.9.2).	✓	✓	✓
3.- Identificación y funciones del/los Responsables de Seguridad (Art.15 y 16).		✓	✓
4.- Trabajo fuera de ubicación principal debe ser expresamente autorizado (Art.6).	✓	✓	✓
5.- Listado de personal con acceso a Servidores y/o CPD (Art.19).		✓	✓
6.- Listado de personal con privilegios administrativos informáticos sobre aplicaciones y ficheros (Art.12.4).	✓	✓	✓
Estructura de los Ficheros y del Sistema Informático:			
1.- Descripción y estructura informática del Fichero (campos ID)	✓	✓	✓



2.- Descripción y estructura del Sistema Informático (enumeración de equipos, redes, programas, etc...)	✓	✓	✓
Gestión de Soportes:			
1.- Identificación, inventariado y almacenamiento (Art.13.1).	✓	✓	✓
2.- Autorización necesaria para salida de soportes (Art.13.2).	✓	✓	✓
3.- Cifrado de soportes en caso de operaciones externas de mantenimiento (Art.20.4).		✓	✓
4.- Medidas y procedimientos para la destrucción de soportes (Art.20.3).		✓	✓
5.- Registro de Entrada de Soportes (Art.20.1).		✓	✓
6.- Registro de Salida de Soportes (Art.20.2).		✓	✓
7.- Distribución de soportes con mecanismos de cifrado de datos (Art.26).			✓
Ficheros Temporales:			
Aplicación de mismo nivel de seguridad que fichero origen (Art.7).	✓	✓	✓
Registro de Incidencias:			
1.- Contenido mínimo: tipo de incidencia, momento en que se produce, efectos producidos, persona que comunica, medidas adoptadas (Art.10).	✓	✓	✓
2.- Contenido adicional: Procedimiento de restauración de datos, datos restaurados y datos grabados manualmente (Art.21.1)		✓	✓
Procedimientos de Copias de Respaldo y Recuperación datos:			
1.- Deberán garantizar la restauración de los datos al	✓	✓	✓



momento anterior a producirse la pérdida (Art.14.2).			
2.- Realización de copias de backup al menos con una frecuencia semanal (Art.14.3).	✓	✓	✓
3.- Necesaria autorización para la ejecución de procedimientos de restauración de datos (Art.21.2).		✓	✓
4.- Almacenamiento externo de copias y procedimientos de restauración de datos (Art.25).			✓
Pruebas con datos reales:			
Aplicación de mismas medidas según nivel de seguridad de los datos (Art.22).		✓	✓
Actualización y Auditoria:			
1.- Revisión y actualización del Documento de Seguridad en función de cambios relevantes en la Organización (Art.8.3).	✓	✓	✓
2.- Auditoria cada 2 años. Conservación de Informe a disposición AEPD (Art.17).		✓	✓
3.- Revisión periódica de la información de control de los accesos informáticos a ficheros y aplicaciones (Art.24.5).			✓



Medidas específicas para datos en soporte papel:			
1.- Control de acceso a la documentación.	✓	✓	✓
2.- Medidas de conservación y almacenamiento.	✓	✓	✓
3.- Procedimientos y mecanismos de destrucción que impidan posterior recuperación de la información que contienen.	✓	✓	✓



**FASES A REALIZAR EN UNA BUENA PROTECCION**

<p>FASE 1.- Análisis de la Organización. Tratamiento de los Datos</p>	<p>Obtener información pormenorizada sobre la organización. Especificación de Ficheros de Datos de Carácter Personal y Sistemas de Información. Procedimientos implantados y los flujos de información.</p>	<p>OBSERVACIONES</p>
<p>PASE 2.- Análisis de los Sistemas Informáticos</p>	<p>Análisis de los Sistemas de la Información en los que se alberga los datos de carácter personal, tanto de los aspectos técnicos como de los procedimientos implantados. Guía de medidas de Seguridad exigidas en el Reglamento de Seguridad que es necesario establecer en función del nivel de seguridad del fichero.</p>	
<p>FASE 3.- Desarrollo De los procedimientos y cobertura legal de la empresa</p>	<p>Desarrollo de los procedimientos que no están actualmente en vigor en la organización, así como la adaptación de los existentes para el cumplimiento de la ley. Redacción y Revisión de todas las cláusulas, formularios, documentos y advertencias legales necesarias para el correcto cumplimiento de la ley. Código de Buenas Practicas de Seguridad Informática para los usuarios del Sistema de Información,</p>	
<p>FASE 4.- Asesoramiento Final Entregables</p>	<p>Registro de los ficheros en la RGPD, Documento de Seguridad, Guía de Obligaciones, Código de Buenas Practicas, Documentación Legal.</p>	