La información ha sido siempre un recurso muy valioso, revalorizado en estos tiempos más aún por el desarrollo la expansión de las Tecnologías de la información y de las comunicaciones. Es por ello que las empresas hoy en día deben dotarse de herramientas y mecanismos de protección y salvaguarda. Mecanismos que permitan proteger la información de robos, intrusiones o accesos deliberados no consentidos, desastres tanto humanos como físicos o naturales, etc., etc.

A parte de lo anteriormente expuesto cabe destacar que la potencia de los ordenadores sobre el papel a la hora de tratar la información que suministran las bases de datos y la generalización de sus uso por cualquiera que tenga un PC, ha obligado a los gobiernos a publicar normas jurídicas que regulen el tratamiento de la información, en consecuencia a los factores que impulsar proteger la información debe añadirse: y para el cumplimiento de ciertos requisitos legales.

Estas normas jurídicas nuevas son de extraordinaria importancia, porque afectan a los derechos fundamentales de la persona. Son los mismos derechos fundamentales que la persona tenía antes de que la informática se introdujera en la vida cotidiana, pero ahora más protegidos, en la medida que las nuevas tecnologías permiten un abuso mayor y más extendido.

En España desde 1978, ***la Constitución española limita el uso de la informática para preservar la intimidad de sus ciudadanos*** en el artículo 18.4. La ley a la que se refiere este aparatado se previo en la misma pero no se dicto hasta que no hizo falta. Lo que ocurrió cuando la informática por la fuerza de la tecnología y el abaratamiento de los sistemas de proceso de la información (hardware y software) resultó tan potente que se hizo un peligro. En 1992 se dicta la ley Orgánica 5/1992 de 29 de Octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter Personal ("LORTAD"). Esta ley ha sido sustituida por la ***ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal ("LOPD"), dictada con el objeto 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, su honor e intimidad personal y familiar.***

Las empresas deben inventariar estos activos y dotarlos de ciertas medidas de protección y seguridad.

DATO: es la unidad mínima de información
INFORMACIÓN: es todo dato o conjunto de ellos que transmiten un conocimiento en un proceso de comunicación entre un emisor y un receptor.
Agregación de datos que tienen un significado especifico más allá de cada uno de éstos. Un ejemplo: 2,0,0 y 1 son datos; 2001 es una información.
HARDWARE: (equipo físico, maquinaria). Componentes físicos de un ordenador o de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar.
SOFTWARE: (componentes lógicos, programas). Programas o elementos lógicos que hacen funcionar un ordenador o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos del ordenador o la red.
TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES (ICT): Una forma de denominar el conjunto de herramientas, habitualmente de naturaleza electrónica, utilizadas para la recogida, almacenamiento, tratamiento, difusión y transmisión de la información.

LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La Ley Orgánica 15/1999, se aplica 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. La Ley considera "dato de carácter personal" a cualquier información concerniente a personas físicas identificadas o identificables. Y protege estos datos en orden a su "tratamiento", que no es otra cosa que 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.

Del conjunto de datos personales son de destacar un tipo de datos que la LOPD califica de "especialmente protegidos". Son los más cercanos al derecho fundamental a la intimidad, en el sentido de que son los que más se aproximan al concepto de zona reservada de los individuos. Estos datos, son los

que se refieren a la ideología, religión, creencias, afiliación sindical, salud, vida sexual, origen racial o étnico y comisión de infracciones penales o administrativas. El legislador trata a este tipo de datos de forma diferenciada ya que entiende que, en principio, todos los datos personales no deberían ser conocidos por nadie si el interesado no lo desea, pero estos datos aún en menor medida deben ser conocidos (a no ser que exista consentimiento del interesado o exista una necesidad de conocerlos para preservar otro derecho de nivel superior a la intimidad, como pudiera ser el derecho a la vida en una situación médica urgente). Estos datos especialmente protegidos tienen un régimen jurídico especial.

La LOPD considera "fichero" todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Cualquier tratamiento de datos está limitado.

Pero no son "fichero" a estos efectos ficheros que posean personas físicas en el ejercicio de sus actividades "exclusivamente personales o domésticas" (por ejemplo, los de una agenda electrónica o PDA), ni :

- Los "sometidos a la normativa sobre protección de materias clasificadas" (por ejemplo, los secretos del CESID).
- Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada, aunque el Ministerio del Interior debe comunicar su existencia y su finalidad a la Agencia de Protección de Datos.
- Muchos ficheros de las Administraciones Públicas, aunque se encuentran protegidos por otro tipo de legislación.

La LOPD se aplica tanto a los datos personales registrados en soporte físico que los haga susceptibles de tratamiento como a toda modalidad de uso posterior de los datos personales llevados a cabo por los sectores público y privado. Es de aplicación a todo tipo de tratamiento (no sólo informático).

Artículo 4. Aplicación de los niveles de seguridad.

1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificada como de nivel básico.
2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas de nivel medio.
3. Los ficheros que contengas datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de los personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.
4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo, deberán garantizar las medidas de nivel medio establecidas en los artículos 18, 18, 19 y 20.
5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

GESTIÓN DE SOPORTES Y COPIAS DE RESPALDO Y RECUPEREACIÓN

NIVEL BÁSICO

Artículo 13 del Reglamento
"1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero."

Por soporte informático, según el artículo 2.10 del Reglamento de Seguridad se entiende a cualquier "objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se puedan grabar o recuperar datos".
Artículo 14 del Reglamento
"1. El responsable del fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos.

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

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

MEDIDAS DE NIVEL MEDIO ATENUADO

El artículo 20 del Reglamento de Seguridad señala lo siguiente:

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

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

3. Cuando un soporte vaya a ser desechado o reutilizado se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él previamente a que se proceda a su baja en el inventario.

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

MEDIDAS DE NIVEL MEDIO

El artículo 21 del Reglamento de Seguridad señala lo siguiente:

"1. En el registro regulado en el artículo 10 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesario la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos."

MEDIDAS DE NIVEL ALTO

El artículo 23 del Reglamento de Seguridad señala lo siguiente:

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

El artículo 25 del Reglamento de Seguridad establece lo siguiente:

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

CONCEPTOS

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

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

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

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

Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento.

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

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.

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.

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

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

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