



# **SEGURIDAD INFORMÁTICA**

**LOPD 15/99**

**LSSI 34/2002**

• Legislación aplicable	2
• Ficheros de datos personales	3
– <b>Nivel Básico</b>	<b>4</b>
– <b>Nivel medio</b>	<b>5</b>
– <b>Nivel alto</b>	<b>6</b>
• Reglamento de Medidas de Seguridad	7
• Medidas de seguridad de nivel básico	8
• Medidas de seguridad de nivel medio	9
• Medidas de seguridad de nivel alto	10
• AEPD (Agencia Española de Protección de Datos)	11
• LSSI	12
• Obligaciones y regímenes de responsabilidad	13
• Autorregulación	15
• Contenidos nocivos	16
• Coloquio final (Ruegos y preguntas)	17

- **LOPD (Ley Orgánica de Protección de Datos)**

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

- **Reglamento de Medidas de Seguridad**

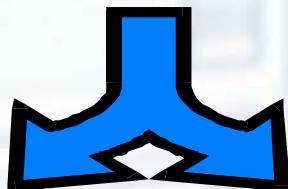
- El Reglamento, aprobado por el Real Decreto 994/1999 de 11 de junio, tiene por objeto el desarrollo de lo dispuesto en la LOPD respecto a las medidas de seguridad a aplicar sobre los ficheros que contienen datos de carácter personal.

- **¿Qué es un DATO PERSONAL?**

Se entiende por “datos de carácter personal” cualquier información concerniente a personas físicas identificadas o identificables:

- Nombre, apellidos, DNI, Dirección, datos bancarios, etc.
- Entre los datos de carácter personal hay unos especialmente sensibles que tiene mayores restricciones según la ley LOPDCP: Ideología, religión o creencias, raza, salud, vida sexual, afiliación sindical...

### ORIGEN



### TITULARIDAD PÚBLICA

- Se crean a través de una disposición oficial publicada en el BOE.
- No es necesario el consentimiento del afectado para la cesión de datos entre administraciones públicas.
- La cesión de datos personales sólo es posible cuando la misma se encuentra prevista dentro de las disposiciones de creación del fichero.

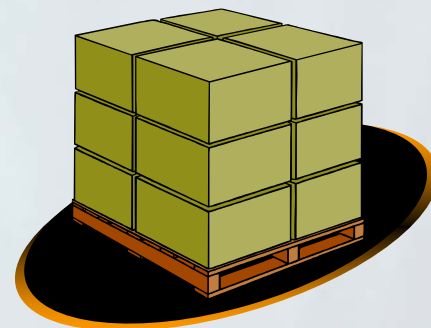
### TITULARIDAD PRIVADA

- Pueden crearse cuando sean necesarios para el logro de la actividad legítima de la empresa.
- Deben ser notificados y registrados ante la Agencia de Protección de Datos.
- La cesión de datos debe ser comunicada a los afectados.

- Las medidas de seguridad requeridas por el Reglamento se clasifican en tres niveles diferentes, dependiendo de la naturaleza de la información tratada y del grado de necesidad de garantizar la confidencialidad e integridad de la información.

**Todos los ficheros que contengan datos de carácter personal deben cumplir las medidas de nivel básico**

### Nivel Básico

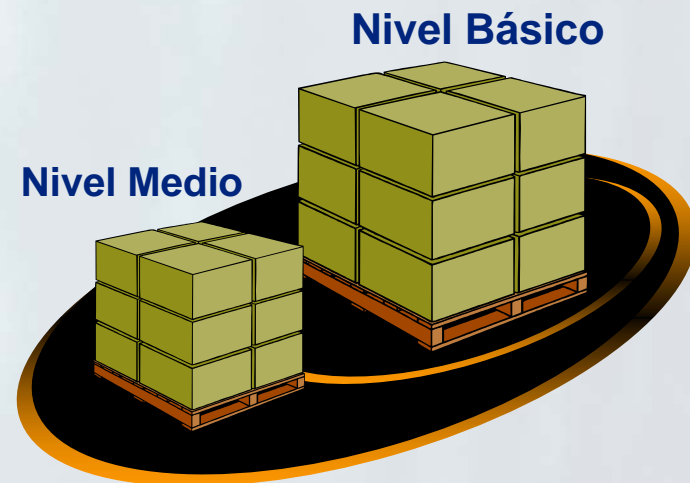




- Las medidas de seguridad requeridas por el Reglamento se clasifican en tres niveles diferentes, dependiendo de la naturaleza de la información tratada y del grado de necesidad de garantizar la confidencialidad e integridad de la información.

Se consideran de **nivel medio** aquellos ficheros que contengan datos relativos a:

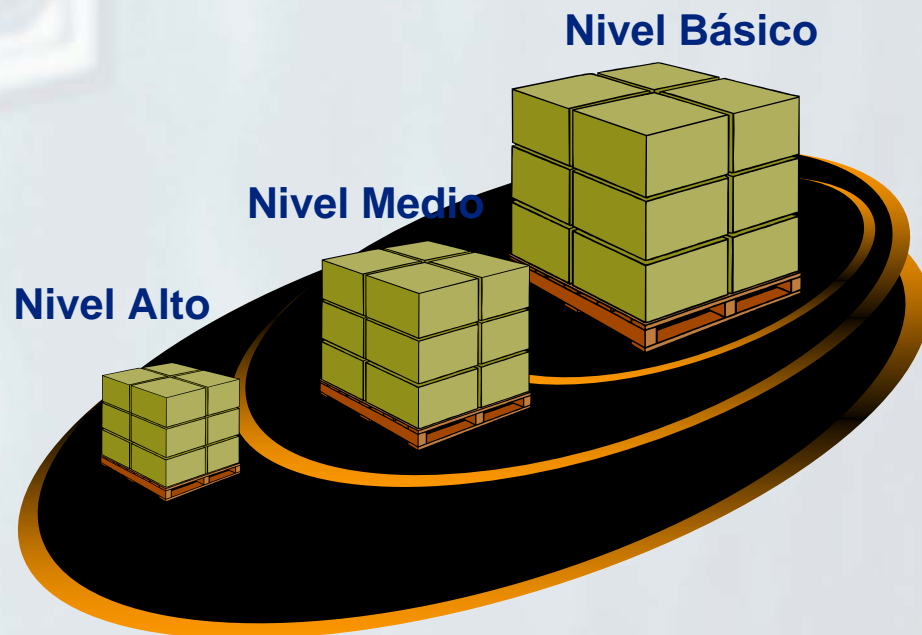
- ✿ Gustos, tendencias, etc. que permitan obtener una evaluación de la personalidad del individuo.
- ✿ Solvencia patrimonial y crédito
- ✿ Hacienda pública
- ✿ Servicios financieros
- ✿ Comisión de infracciones administrativas o penales



- Las medidas de seguridad requeridas por el Reglamento se clasifican en tres niveles diferentes, dependiendo de la naturaleza de la información tratada y del grado de necesidad de garantizar la confidencialidad e integridad de la información.

Los ficheros considerados de **nivel alto** son aquellos que contienen datos relativos a:

- ✿ Ideología
- ✿ Religión
- ✿ Creencias
- ✿ Origen Racial
- ✿ Salud
- ✿ Vida sexual
- ✿ Datos recabados para fines policiales sin consentimiento de las personas afectadas



- El reglamento se estructura en una serie de disposiciones generales que se han de cumplir independientemente de la clasificación de los datos para luego pasar a describir las medidas específicas de cada uno de los niveles de clasificación.
- Las medidas recogidas en el reglamento son de tipo técnico y organizativo, aunque algunas de ellas requieren la combinación de ambas, por ejemplo:
  - Medidas técnicas
    - Limitación del número de intentos de acceso no autorizados al sistema.
    - La transmisión de datos personales a través de redes de Telecomunicaciones debe realizarse de forma cifrada.
  - Medidas Organizativas
    - Existencia de la figura del responsable de seguridad.
    - Almacenamiento de los backups y los procedimientos de recuperación en un lugar diferente al edificio donde se encuentran los equipos informáticos.
  - Medidas conjuntas
    - Identificación inequívoca y personalizada de todos los usuarios que intenten acceder al sistema.



- Independientemente del nivel de los datos tratados, el reglamento establece que:
- Las medidas de seguridad para el tratamiento de datos a través de **redes de comunicaciones** deberán garantizar un **nivel de seguridad equivalente a** los accesos en **modo local**.
  - Cuando se **trabaje** con los ficheros **fuera de los locales** en los que se ha declarado que se realiza su tratamiento, éste **deberá ser autorizado** y llevarse a cabo garantizando los **mismos niveles de seguridad**.
  - Cuando se trabaje con **ficheros temporales**, éstos deberán ser **borrados una vez finalizada su utilidad** y durante su existencia deberán tener las **mismas medidas de seguridad** que los originales de los que han sido extraídos.

- Las medidas incluidas en el Reglamento de Seguridad para el nivel básico son:
  - Existencia de un **documento de Seguridad**.
  - Existencia de un **documento** en el que se encuentren claramente definidas y documentadas las **funciones del personal con acceso a los datos** de carácter personal.
  - Existencia de **mecanismos de control de acceso** a datos personales:
    - Los usuarios deben tener acceso únicamente a los datos que necesitan para el desempeño de sus funciones.
    - Los mecanismos deben evitar el acceso a datos no autorizados.
    - Si el mecanismo de autenticación es usuario y contraseña debe existir un procedimiento para su gestión y cambio
    - Debe existir una relación de usuarios con los accesos autorizados.
    - Únicamente personal autorizado puede conceder y modificar los derechos de acceso.
  - Existencia de una **gestión de soportes** (cintas, cartuchos, discos) con datos de carácter personal que permita identificar, inventariar y almacenar la información.
  - Existencia de un registro de **incidencias**.
  - Existencia de **procedimientos** de generación y recuperación de **copias de seguridad**.
    - Deberán realizarse copias de respaldo, como mínimo, semanalmente.
  - Deberá contener al menos, el tipo de incidencia, el momento en el que se produjo y la persona que realiza la notificación.

- Para los ficheros clasificados como de nivel medio se deben respetar todas las medidas de nivel básico y además:
  - Existencia de la figura del **responsable de seguridad**
  - Realización de **Auditorías** cada 2 años
  - **Identificación inequívoca** y personalizada de todos los usuarios que intenten acceder al sistema
  - **Limitación** del número de **intentos de acceso** no autorizados al sistema
  - Existencia de **control de acceso físico** a los locales dónde están ubicados los sistemas de información con datos de carácter personal
  - Debe **registrarse la información** del tipo fecha, origen, información, destinatario, ..., en la **entrada y salida de soportes** con datos de nivel medio
  - Deben **registrarse los procedimientos** realizados **para la recuperación** de los datos, quién los ha ejecutado y qué datos se han modificado, en la resolución de incidencias
  - Además, en el **registro de incidencias** deberán incluirse los **procedimientos de recuperación**
  - **No** se pueden realizar **pruebas** de desarrollo **con datos reales**

- Para los ficheros clasificados como de nivel alto, además de las medidas de seguridad de Nivel Básico y Medio, deben cumplirse las medidas citadas a continuación:
  - Los datos de carácter personal de nivel alto deben **cifrarse para su distribución** en soportes
  - Debe **registrarse, en los accesos a datos personales**, la siguiente información: usuario, fecha, hora, fichero accedido, tipo de acceso y si ha sido autorizado o denegado
    - Los datos registrados se deben conservar como mínimo 2 años
    - El responsable de seguridad deberá tener control directo de los mecanismos de registro, revisar los registros periódicamente y elaborar un informe de problemas detectados en las revisiones.
  - **Almacenamiento de las copias** de seguridad y los procedimientos de recuperación en un **lugar diferente** al lugar donde se encuentran los equipos informáticos
  - La **transmisión** de datos personales a través de redes de Telecomunicaciones (tanto públicas como privadas) debe realizarse **de forma cifrada**

- Función de la AEPD:

- Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- Ejerce de potestad sancionadora:
  - Las sanciones van de las 600 euros (100.000 pts) hasta los 600.000 euros (100MM pts) en función de la gravedad de la infracción.



- Sanción de 60.101 € (10 MM pts) por envío de un correo electrónico publicitario a un particular, cuando éste había manifestado que no quería recibir publicidad.
- Procedimiento sancionador en curso contra diversas entidades financieras por un posible mal uso de datos confidenciales de sus clientes con multas de hasta 601.012 € (100 MM pts), tras recibir la denuncia de haber encontrado datos de clientes en contenedores de basura próximos a algunas oficinas de estas Entidades.
- Sanción de 60.101 € (10 MM pts) por facilitar el número de teléfono de un cliente a un comercio que lo solicita para resolver un error producido en el pago con tarjeta a favor del cliente.
- Sanción de 60.101 € (10 MM pts) por facilitar el saldo de una cuenta a una persona sin ser titular (hermano).

- **LSSI: Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la información y de Comercio Electrónico**
  - Entró en vigor el 12 de Octubre de 2002
  - Creada a partir de la Directiva de Comercio Electrónico aprobada por la UE en el 2000.
  - Regula el régimen jurídico de los **servicios de la sociedad de la información** y de la **contratación por vía electrónica**.
  - **Se aplica** a servicios onerosos o gratuitos **siempre** que suponga una **actividad económica para el prestador del servicio**.

- Comunicación al Registro Mercantil (u otro registro público) de un nombre de dominio o dirección de Internet
- Mostrar en su página web: Denominación social, NIF, Domicilio, correo electrónico, inscripción en el Registro Mercantil u otro Registro público, autorización administrativa a la que está sujeta su actividad e identificación del órgano competente encargado de su supervisión.
- Si ejerce una profesión regulada: Colegio profesional, núm. colegiado, título académico, estado en que se expidió y normas profesionales aplicables al ejercicio de su profesión
- Información clara y exacta sobre el precio de los productos y servicios que ofrece
- Códigos de conducta a los que estén adheridos

- Los **prestadores** de servicios tienen la **obligación de suspender** la transmisión, el alojamiento de datos, al acceso a las redes o la **prestación** de cualquier servicio **cuando** éste contenga **contenidos ilícitos**.
- Los **operadores y proveedores** de servicios **guardarán los datos** generados por las comunicaciones, que sean **necesarios para** facilitar la **localización del equipo terminal empleado por el usuario para la transmisión de información**, por un periodo de 12 meses.
- Los **prestadores de servicios** de la sociedad de la información está sujetos a **responsabilidad: civil, penal y administrativa**.

- La autorregulación se fomenta en España a instancia de la directiva europea de tres maneras:
  - **Línea Directa (hot-line):** centros de denuncia creados por los proveedores por teléfono o e-mail. No tienen potestad sancionadora, pasan la denuncia a la Policía.
  - **Códigos de Conducta:** las Admones. Pbcas impulsan códigos voluntarios por parte de asociaciones u organizaciones comerciales, profesionales y de consumidores. La Admón General Central del Estado fomentará códigos de conducta de ámbito comunitario o internacional.
- En España está el Código de Confianza on-line. Las empresas que actúan según él reciben un sello de calidad.
  - **IQUA:** Agencia de calidad de internet.



- Los contenidos nocivos son diferentes a los ilegales pues están dentro del marco legal, por ejemplo contenidos pornográficos para adultos.
- La práctica habitual es el uso de filtros aunque la LSSI no prevé esta obligación pero sí presupone la existencia de este método.
- Respecto a los contenidos nocivos la LSSI necesita medidas complementarias como la autorregulación de los proveedores o el control paternal.

# Deloitte.