

UT_2 LEGISLACION

NORMATIVA DE LOS DATOS PERSONALES

1.- LEY ORGANICA 15/1999 LOPD

El Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

- GDPR (General Data Protection Regulation)
- RGPD (Reglamento General de Protección de Datos) es la nueva normativa que regula la protección de los datos de los ciudadanos que vivan en la Unión Europea. El reglamento entró en vigor el 24 de mayo de 2016, pero es de obligado cumplimiento a partir del 25 de mayo de 2018.
- Esta nueva normativa determina que todas las empresas, independientemente de su país de origen o de actividad, deberán cumplirla si recogen, guardan, tratan, usan o gestionan algún tipo de dato de los ciudadanos de la Unión Europea.
- Para que una empresa pueda utilizar estos datos, tendrás que dar tu consentimiento. Pero ya no se hará como hasta ahora, cuando las empresas suelen utilizar largos términos ilegibles y condiciones plenas de jerga legal.

<https://www.boe.es/buscar/doc.php?id=BOE-A-2018-10751>

- Protege los datos de carácter personal
- Todas las empresas deben cumplirlo o se arriesgan a tener sanciones de la agencia de protección de datos
- Establece obligaciones destinadas a proteger los datos
 - Tanto en soporte electrónico
 - Soporte físico o papel
- Ámbito de aplicación
 - Datos de carácter personal pertenecientes a una persona física identificada o identificable
 - Ficheros. conjuntos organizado de datos de carácter personal, cualquiera que sea la forma y modalidad de su tratamiento
 - Tratamiento. Son operaciones y procedimientos técnicos de carácter automatizado sobre los datos, elaboración, conservación y transmisión.

2.-AGENCIA ESPAÑOLA DE PROTECCION DE DATOS

- Todos los ficheros que contenían datos, se comunicaban a la agencia española de protección de datos hasta mayo de 2018: www.aepd.es.
- <https://www.aepd.es/herramientas/inscripcion-ficheros.html>
- La obligación de notificar ficheros se sustituye a partir del 25 de mayo de 2018 por elaborar un registro de actividades de

tratamiento que deberá contener la información señalada en el artículo 30 del citado Reglamento.

- Algunas comunidades tienen regulación propia

3.-TRATAMIENTO DE LOS DATOS

- El tratamiento de los datos está determinado por la ley para evitar abusos y usos ilícitos
- La recogida de datos requiere informar al usuario de :
 - Titular del fichero
 - Finalidades del tratamiento
 - Carácter obligatorio de las respuestas por parte de la empresa
 - Derechos y posibilidades de ejercerlos
 - Acceso
 - Rectificación
 - Cancelación
 - Oposición
 - Dirección y condiciones para ejercer tales derechos
- La ley establece unas obligaciones para garantizar el correcto tratamiento de los datos por parte del responsable del fichero
- El interesado siempre podrá revocar el consentimiento dado.

4.-NIVELES DE SEGURIDAD DE LOPD

- Siempre que se vaya a crear un fichero de datos de carácter personal, es necesario solicitar la aprobación de la AGPD.
- Depende de los datos se debe establecer por ley unos niveles de seguridad como :
 - Elaboración de un documento de seguridad en el que se detallan los datos almacenados.
 - Las medidas de seguridad adoptadas.
 - Personas que tienen acceso a esos datos.
- La ley establece tres niveles
 - **Nivel básico** : datos de carácter personal(nombre apellidos, dirección teléfono, etc)
 - **Nivel medio**: infracciones penales, infracciones administrativas, hacienda pública, servicios financieros
 - **Nivel alto**: ideología, religión, creencias, origen racial, etc
- Cada nivel tienes sus propias protecciones
 - **Básico**
 - Documento de seguridad con funciones y obligaciones de cada empleado
 - Registro de incidencias del fichero.
 - Identificación y autenticación de usuarios

- Gestión de soportes- destrucción de cualquier soporte con datos desechado
- Copias de seguridad como mínimo una vez a la semana
- **Medio**
 - Las medidas del nivel básico.
 - Se hacen auditorias
 - Medidas adicionales de identificación y autenticación
 - Medidas de control de acceso físico
- **Alto**
 - Medidas de nivel bajo y medio
 - Datos cifrados
 - Registro de acceso de los dos últimos años como mínimo
 - Copias de seguridad almacenadas en lugar diferente a donde se encuentran los equipos.

Comprobar cuales son las funciones de estas webs:

<https://clickdatos.es/>

Buscar información acerca de la petición al **derecho a olvido**

Ley de servicio de sociedad de la información y de comercio electrónico (LSSI-CE)

- Ley 34/2002.
- Regula las situaciones de comercio electrónico.
- Siempre que se reciba un ingreso económico a través de un medio telemático dicha actividad entra en los ámbitos de aplicación de la ley.
- Las empresas están obligadas a publicar en la web los siguientes datos
 - Nombre de la empresa o denominación social, domicilio,.
 - Nif/cif
 - Correo electrónico
 - Precio del servicio.
 - Razón social
 - Todo ello de forma muy clara
- Las empresas que incumplan la presentación de dicha información pueden tener infracciones graves, muy graves o leves que pueden ir de 30000 a 600000

Comunicaciones comerciales

- Identificar de forma clara el nombre de la persona física o jurídica en nombre de la que envía el mensaje publicitario.
- Incluir en el comienzo del mensaje la palabra "Publicidad" (en los correos electrónicos o "Publi" (en los SMS).

- Facilitar al receptor del mensaje la posibilidad de revocar el consentimiento de una forma sencilla y gratuita.

La ley de propiedad intelectual (LPI)

Establece los derechos de autor en los entornos digitales.

La administración electrónica pretende resolver por internet varios trámites

- **Disponibilidad 24 horas.** Se puede hacer incluso en días festivos.
- **Facilidad de acceso.** Los portales de la Administración proporcionan múltiples asistentes para ayudar.
- **Ahorro de tiempo,** no hay que desplazarse hasta la oficina y esperar turnos.
- **Fiabilidad.** Los procedimientos dependen del sistema.

Administración Electrónica

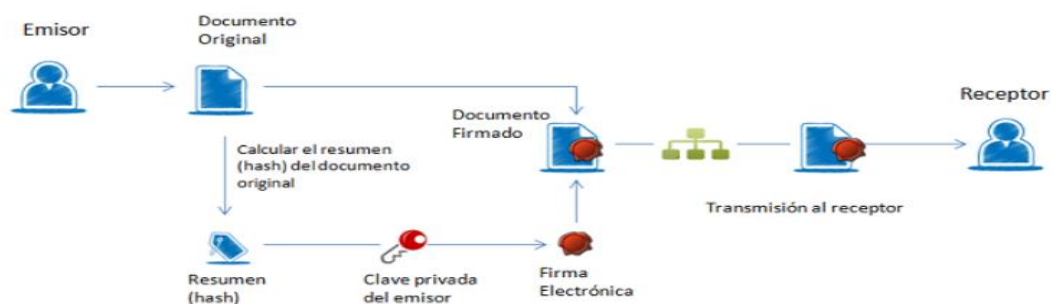
La **Administración Electrónica** hace referencia al esfuerzo de todos los estamentos públicos para adaptar sus procedimientos a las nuevas tecnologías.

Firma electrónica es el “conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medios de identificación del firmante”.

Funciones básicas son:

- **Identificar al firmante de manera inequívoca**
- **Asegurar la integridad del documento firmado.** Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación
- **Asegurar el no repudio del documento firmado.** Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento

Firma electrónica



1. El usuario dispone de un documento electrónico y de un certificado que le pertenece y le identifica.
2. La aplicación utilizada para la firma realiza un resumen del documento. Este resumen es único y cualquier modificación del documento implica también una modificación del resumen.
3. La aplicación utiliza la clave privada para codificar el resumen.
4. La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este nuevo documento es la firma electrónica.

Por su parte, el **certificado digital o electrónico** es un fichero físico mediante el cual se identifica una persona en Internet.

- Expedido por una **Autoridad de Certificación**
- Tiene como misión **validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta**.
- Contiene la información necesaria para firmar electrónicamente e identificar a su propietario con sus datos: nombre, NIF, algoritmo y claves de firma, fecha de expiración y organismo que lo expide.
- La Autoridad de Certificación da fe de que la firma electrónica se corresponde con un usuario concreto.
- En un Certificado, las claves digitales son los elementos esenciales para la firma e identificación del firmante. Existen dos claves, la clave privada y clave pública, y trabajan de forma complementaria. Lo que cifra o codifica una clave sólo lo puede descifrar o decodificar la otra.

Ejemplos de certificados digitales:

- DNle → DNI Electrónico
- FNMT → Fábrica Nacional de Moneda y Timbre