***Imagen que contiene Logotipo

Descripción generada automáticamente***

Alejandro Ortega Martínez

Grado en Ingeniería Informática

12/3/2021

Trabajo 1

Asociación Española de Protección de Datos

Diseño y Administración de Sistemas y Redes

Contenido

[1. Protección de Datos 3](#_Toc66386410)

[1.1. ¿Qué es la Protección de Datos? 3](#_Toc66386411)

[1.2. ¿Qué entendemos por datos personales? 3](#_Toc66386412)

[1.2.1. Tipos de datos personales 4](#_Toc66386413)

[2. Historia de la Protección de Datos 5](#_Toc66386414)

[2.1. Edad antigua: Grecia y Roma 5](#_Toc66386415)

[2.2. Edad Media 5](#_Toc66386416)

[2.3. Edad Moderna: La razón 5](#_Toc66386417)

[2.4. Protección de Datos en España 6](#_Toc66386418)

[2.4.1. Previa a la Constitución del 78 6](#_Toc66386419)

[2.4.2. Posterior a la Constitución del 78 6](#_Toc66386420)

[3. LOTARD y LOPD 7](#_Toc66386421)

[3.1. LORTARD 7](#_Toc66386422)

[3.2. LOPD 7](#_Toc66386423)

[3.2.1. Titulo 1: Ley LOPD 7](#_Toc66386424)

[3.2.2. Titulo 2: Principios 7](#_Toc66386425)

[3.2.3. Titulo 3: Derechos de las personas 8](#_Toc66386426)

[3.2.4. Titulo 4: Disposiciones sectoriales 8](#_Toc66386427)

[3.2.5 Titulo 5: Movimiento internacional de datos 8](#_Toc66386428)

[3.2.6. Titulo 6: Órgano de Control 9](#_Toc66386429)

[3.2.7. Titulo 7: Infracciones y sanciones 9](#_Toc66386430)

[4. Asociación Española De Protección de Datos 10](#_Toc66386431)

[4.1 ¿Que es la AEPD? 10](#_Toc66386432)

[4.2 Derechos 11](#_Toc66386433)

[4.2.1. Derecho de acceso 11](#_Toc66386434)

[4.2.2. Derecho de rectificación 11](#_Toc66386435)

[4.2.3. Derecho de Oposición 11](#_Toc66386436)

[4.2.4. Derecho de supresión (“al olvido”) 11](#_Toc66386437)

[4.2.5. Derecho a la limitación del tratamiento 12](#_Toc66386438)

[4.2.6. Derecho a la portabilidad 12](#_Toc66386439)

[4.2.7. Derecho a no ser objeto de decisiones individuales automatizadas 12](#_Toc66386440)

[4.2.8. Derecho de Información 12](#_Toc66386441)

[4.2.9. Derechos Schengen 13](#_Toc66386442)

[4.3. Deberes 13](#_Toc66386443)

[4.3.1. Ejemplos de Medidas de Cumplimiento 13](#_Toc66386444)

[4.3. Donde y como actúa la AEPD 17](#_Toc66386445)

[4.3.1. Internet y redes Sociales 17](#_Toc66386446)

[4.3.2. Publicidad no deseada 17](#_Toc66386447)

[4.3.3. Violencia de género y violencia digital 18](#_Toc66386448)

[4.3.4. Protección de datos y Coronavirus 19](#_Toc66386449)

[4.3.5. Educación y menores 19](#_Toc66386450)

[4.3.6. Videovigilancia 19](#_Toc66386451)

[4.4. Herramientas que proporciona la AEPD 20](#_Toc66386452)

[4.4.1. Facilita RGPD 20](#_Toc66386453)

[4.4.2. Canal del Delegado de Protección de Datos 20](#_Toc66386454)

[4.4.3. Gestiona EIPD 20](#_Toc66386455)

[4.4.4. Facilita Emprende 21](#_Toc66386456)

[4.4.5. Comunica-Brecha RGPD 21](#_Toc66386457)

[5. Ejemplos de sentencias 22](#_Toc66386458)

[5.1. Multa a la Mutua Madrileña (Procedimiento nº.: PS/00586/2017) 22](#_Toc66386459)

# Protección de Datos

## ¿Qué es la Protección de Datos?

La “protección de datos”, según el panhispánico de la rae, es el conjunto de medidas para garantizar y proteger los datos de carácter personal, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, a los efectos de garantizar, en especial, el honor y la intimidad personal y familiar.

En resumen, podemos entender la protección de datos como una **disciplina jurídica** que **nos protege frente a la colección y empleo de nuestros datos personales**, que pueden ser usados para valorar ciertos aspectos de nuestra personalidad (hábitos, relaciones personales, opiniones), asegurando así el honor de los ciudadanos.

## ¿Qué entendemos por datos personales?

Para entender que son los datos personales, empezaremos por aclarar algunos conceptos:

* **Dato**: Antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad. Se encuentra en un documento o soporte (tanto físico como lógico) con calidad de testimonio.
* **Documentación**: Conjunto de datos, noticias o pruebas que se refieren a un determinado asunto.
* Cuando el dato o documentación son sometidos a un tratamiento o adecuación a un fin para obtener un resultado elaborado se convierte en **información**.



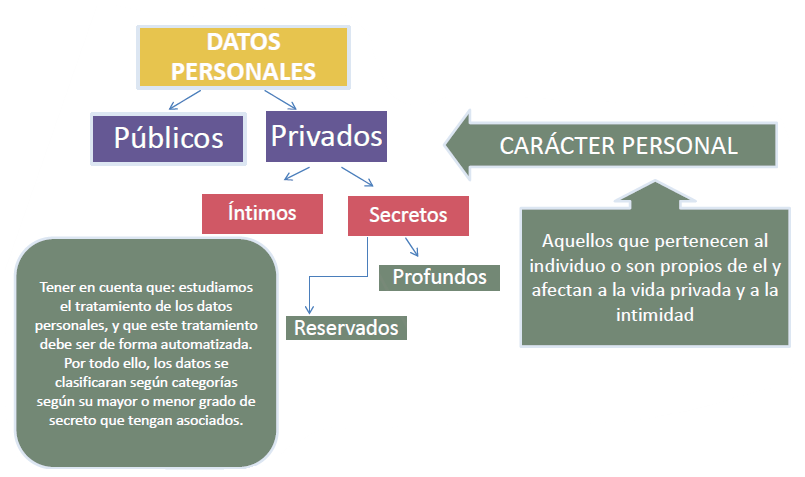
### 1.2.1. Tipos de datos personales

Los datos personales pueden ser de dos tipos:

* **Públicos:** Son aquellos datos personales conocidos por un numero cuantioso de personas.
* **Privados:** Aquellos que tienen regulados y tasadas las situaciones en que la persona está obligada a proporcionarlos.

Dentro de estos últimos, los datos personales privados, tenemos otras dos subcategorías:

* **Íntimos:** aquellos datos que el titular debe proporcionar regularmente en el cumplimiento de sus obligaciones cívicas.
* **Secretos:** son aquellos datos que el ciudadano no está obligado a revelar, salvo excepciones reguladas en las leyes. Dentro de este grupo hay dos subgrupos:
  + **Reservados:** Aquellos que bajo ningún concepto el titular está obligado a dar a conocer; sin excepciones. (ideología, religión, creencias)
  + **Profundos:** Aquellos que bajo ningún concepto el titular está obligado a dar a conocer, salvo excepciones (leyes). (salud, orientación sexual)



# Historia de la Protección de Datos

Aunque este sea un tema que parece que es relativamente nuevo**, la protección de datos algo que siempre, de alguna manera, ha estado con nosotros**.

## 2.1. Edad antigua: Grecia y Roma

**En Grecia se tenía un concepto distinto de lo que era la privacidad**: para ellos lo importante era la polis (la ciudad), la comunidad, no el individuo.

Sin embargo, en Roma se dan cuenta de que esto no tiene que ser así. Al tener esclavos, se dan cuenta de que efectivamente pueden poseer su cuerpo, pero “no pueden poseer” su mente. Se dan cuenta de que hay un hombre interior y un hombre exterior, es la existencia de este hombre interior, lo que **da lugar en Roma al derecho de propiedad del yo**, y lo que posteriormente derivara en la privacidad.

## 2.2. Edad Media

El concepto de la propiedad del yo sigue avanzando, y son diferentes pensadores de la época los que le van dando alguna vuelta de tuerca y matizando.

Aparece San Agustín, que nos habla del **hombre como portador de valores eternos**, refiriéndose a ese conjunto de “cualidades” privadas de la persona.

Mas adelante llega Santo Tomás, que se da cuenta de que cuando el hombre está rezando, se **produce un momento de intimidad que debe ser sagrado**, sentando así precedentes para la posterior valoración de la intimidad.

A partir de esto, vemos como aparece el “**pater familias**”, donde vamos dando ya forma a la intimidad: se considera a la familia como un único ser, en la que el padre de familia es quien goza de esa primitiva privacidad.

## 2.3. Edad Moderna: La razón

A este concepto de la privacidad se le sigue dando vueltas, hasta que en la edad moderna aparecen los filósofos de la razón, que debatirán sobre estos temas.

Locke desarrolla la idea de la “**libertad negativa**”, donde **reconoce al individuo una esfera intima**, lo cual significa que es el individuo el que ha de tener un “espacio” al que nadie mas puede acceder.

En especial, Jean-Jacques Rousseau, es el primero que nos habla ya de la **intimidad desde el ámbito de la persona**.

1 Jean-Jacques Rousseau

## 2.4. Protección de Datos en España

### 2.4.1. Previa a la Constitución del 78

Para hablar de la protección de datos en España, Nos remontaremos a la edad media.

La primera vez que oímos hablar de algo parecido a la privacidad, es en el 11 de Enero de 1541, con Carlos 1, que nos habla de la **Inviolabilidad de las Cartas\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

Durante mucho tiempo se avanza muy poco, hasta llegar a la Constitución del gobierno provisional de 1869, el previo a la primera república, donde además de la inviolabilidad del correo que ya teníamos, aparece la **inviolabilidad del domicilio y el secreto de los efectos personales**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*.

Mas adelante, en el Fuero de los españoles del 17 de Julio de 1945, aparece en su titulo preliminar el **respeto a la dignidad y libertad humanas como principio fundamental\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*.**

### 2.4.2. Posterior a la Constitución del 78

Cuando llegamos a esta Constitución, ya empieza a aparecer, en el articulo 18.4, donde se va esbozando un poco el tema de la privacidad, y a partir del cual, y con base a este, empiezan a aparecer leyes:

* Ley Orgánica 1/1982 (5 Mayo): Esta ley estipula la **protección civil del derecho al honor,** a la **intimidad personal y familiar**, y a la **propia imagen.**
* Ley 16/1985: Es la ley de patrimonio histórico Español, pero también se tocan temas de privacidad.
* Ley 13/1986: Es la ley de Fomento y coordinación general de la investigación científica y tecnológica. En esta ley se tocan temas sobre **hasta donde podemos llegar con la investigación de los datos de las personas**.
* Ley 12/1989: Regula la función estadística pública

Todo esto sirve de antecedente para cuando, en 1992, aparece la **Ley Orgánica de Protección de Datos,** de la que hablaremos más adelante.

# 3. LOTARD y LOPD

## 3.1. LORTARD

La Ley Orgánica 5/1992, del 29 de Octubre, de regulación del tratamiento Automatizado de los datos de carácter personal (LOTARD), surgió como el fruto de desarrollar el articulo 18 de la Constitución Española de 1978 y establece, por primera vez, la limitación del uso de la informática para garantizar la intimidad personal.

La LOTAD tardó siete años en disponer de su desarrollo reglamentario, que llegó con el decreto 994/1999 del 11 de Junio: el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal (RMS).

Pocos meses después de este lanzamiento, con el objetivo de ampliar esta ley y adaptarla a la Directiva europea, nace la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

## 3.2. LOPD

Es la **ley que se encuentra vigente hoy en día**, y consta de 49 artículos agrupados en 7 títulos y finalizado con 6 disposiciones adicionales, 3 disposiciones transitorias, 1 derogatoria y 3 finales. A continuación se hará un breve resumen de los siete títulos.

### 3.2.1. Titulo 1: Ley LOPD

El **objetivo** de este título es **garantizar y proteger el tratamiento de datos personales**, y se aplica a los datos de carácter personal registrados en soporte físico susceptibles de tratamiento y uso posterior por los sectores público y privado.

Sin embargo, hay algunos **ficheros regulados según legislación específica**, como ficheros con fines estadísticos (Legislación del régimen electoral), ficheros de informes de calificación del régimen personal de las fuerzas armadas, ficheros del registro civil y del registro de penados y rebeldes, y de imágenes y sonidos de videocámaras de las fuerzas y cuerpos de seguridad.

### 3.2.2. Titulo 2: Principios

* **La calidad de los datos:** Exactitud, puesta al día, pertinencia, posibilidad de utilización, almacenamiento.
* **El derecho de información** al dueño de los datos de la existencia del fichero, derecho al acceso de datos, conocimiento de los datos y a exigir cancelación o rectificación.
* **El principio de consentimiento**

También regula los requisitos de **El deber de secreto de los responsables del fichero**, y de la **cesión de datos**, entendiendo por esto que solo se pueden “dar los datos a terceros” con una finalidad de tratamiento de estos datos, mas que para cumplimiento de fines directamente relacionados con funciones legítimas.

### 3.2.3. Titulo 3: Derechos de las personas

* **Derecho de Impugnación**: Los ciudadanos tienen derecho a no verse sometidos en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. Podrán impugnar un tratamiento de datos que ofrezca una definición de sus características o personalidad.
* **Derecho información y acceso del afectado** respecto a sus datos de carácter personal (más de 12 meses).
* **Derecho de rectificación y cancelación**: datos inexactos, incompletos o no adecuados. (10díashábiles)
* **Indemnización**: Cuando sufra daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en esta Ley.

### 3.2.4. Titulo 4: Disposiciones sectoriales

Se clasifican en dos:

* **Ficheros de titularidad pública:** Su creación, modificación o supresión solo podrán llevarse a cabo por medio de disposición general publicada en el BOE o en el diario oficial correspondiente.
* **Ficheros de titularidad privada:** Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías. Se exige siempre el consentimiento del interesado para recabar los datos.

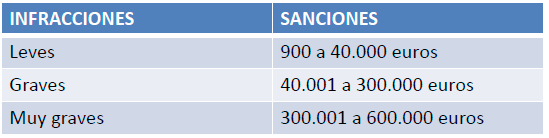
### 3.2.5 Titulo 5: Movimiento internacional de datos

Regula la transferencia de datos personales de un Estado a otro, de acuerdo con la protección existente en el destino, que debe ser equiparable a la que presenta la ley. Establece los limites de garantía y seguridad en la transmisión telemática o en la transferencia de los datos cruzando fronteras.

### 3.2.6. Titulo 6: Órgano de Control

Estipula a la **Agencia Española de Protección de Datos** como órgano independiente con capacidad de obrar y potestad inspectora. Hablaremos de ella mas adelante

### 3.2.7. Titulo 7: Infracciones y sanciones



* **Leves** (Prescriben al año)**:** Son el incumplimiento del deber de informar al afectado acerca del tratamiento de sus datos de carácter personal, o no remitir a la AEPD las notificaciones previstas en la ley.
* **Graves** (Prescriben a los 2 años): Podrían ser Creación de ficheros sin autorización o sin BOE, tratamiento de Datos sin consentimiento, vulnerar el secreto, impedir el acceso y rectificación, o violar la cesión de datos.
* **Muy Graves** (Prescriben a los 3 años): Recogida de datos de forma engañosa, tratamiento de datos sensibles, no cesar en el tratamiento de datos, o la transferencia de datos a países con menor protección legal que en España.

# 4. Asociación Española De Protección de Datos

## 4.1 ¿Que es la AEPD?

La Asociación Española de Protección de Datos (AEPD) **es la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de los ciudadanos.** Fue fundada Con la salida de la LOPD, en 1999, y sus funciones son las siguientes:

* **Atender peticiones y reclamaciones** de personas afectadas
* **Informar** a los interesados **sobre sus derechos y deberes** en esta materia.
* Tiene **potestad sancionadora**.
* Tiene la capacidad de **controlar y adoptar** las autoridades que procedan en relación con los **movimientos internacionales de datos**.
* Debe **velar por el cumplimiento de la legislación** en materia de protección de datos.



## 4.2 Derechos

En este apartado veremos los derechos que ampara la AEPD.

### 4.2.1. Derecho de acceso

Este derecho se basa en que puedes dirigirte al responsable del tratamiento para conocer si está tratando o no tus datos de carácter personal, y en el caso de que así sea, obtener la siguiente información:

* Una copia de los datos que se están tratando, así como su categoría.
* Los fines del tratamiento, y los destinatarios a los que serán comunicados.
* El plazo previsto de conservación de estos datos.
* Poder presentar una reclamación ante una Autoridad de Control.
* Información sobre de donde han obtenido tus datos.
* La existencia de decisiones automatizadas (elaboración de perfiles, lógica aplicada, etc)
* Si se transfieren los datos personales a terceros países, ser informado de las garantías con las que se transfieren.

### 4.2.2. Derecho de rectificación

Este derecho significa que puedes pedir que se rectifiquen los datos que hayan obtenido de ti que sean inexactos, o que se completen los datos personales que sean incompletos.

### 4.2.3. Derecho de Oposición

Supone que te puedes oponer a que el responsable realice un tratamiento de los datos personales:

* Cuando sean objeto de tratamiento basado en una misión de interés publico o en el interés legítimo, incluido la elaboración de perfiles.
* Cuando el tratamiento tenga como finalidad la mercadotecnia directa, incluida también la elaboración de perfiles anteriormente citada.

### 4.2.4. Derecho de supresión (“al olvido”)

Este derecho se podrá ejercitar cuando ocurra alguno de los siguientes casos:

* Si tus datos personales ya no son necesarios en relación con los fines para los que fueron recogidos.
* Si retiras tu consentimiento al responsable para tratar tus datos.
* Si te has opuesto al tratamiento de tus datos personales al ejercitar el derecho de oposición.
* Si tus datos personales han sido tratados ilícitamente.

### 4.2.5. Derecho a la limitación del tratamiento

Este derecho consiste en que obtenga la limitación del tratamiento de tus datos que realiza el responsable. Puedes solicitar la suspensión del tratamiento:

* Cuando impugnes la exactitud de tus datos.
* Cuando te hayas opuesto al tratamiento que el responsable realiza n base al interés legítimo o misión de interés público, mientras aquel verifica si estos motivos prevalecen sobre los tuyos.

Puedes solicitar al responsable la conservación de tus datos:

* Cuando el tratamiento sea ilícito y te has opuesto a la supresión de tus datos y en su lugar solicitas la limitación de su uso.
* Cuando el responsable ya no necesite los datos, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

### 4.2.6. Derecho a la portabilidad

Este derecho se promulga con la finalidad de reforzar mas el control de los datos personales, de forma que cuando el tratamiento de estos se realice por medios automatizados, recibas tus datos personales en un formato estructurado, de uso común, y puedas transmitirlos a otro responsable del tratamiento.

### 4.2.7. Derecho a no ser objeto de decisiones individuales automatizadas

Este derecho pretende garantizar que no seas objeto de una decisión basada únicamente en el tratamiento de tus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre ti o te afecte significativamente de forma similar.

Sin embargo, este derecho no será aplicable cuando sea necesario para la celebración o ejecución de un contrato entre tu y el responsable, o cuando el tratamiento de tus datos se fundamente en tu consentimiento prestado previamente.

### 4.2.8. Derecho de Información

Debes de ser informado cuando se recaban tus datos de carácter personal, el responsable debe cumplir con este derecho. Debes de ser informado de lo siguiente:

* La identidad del responsable del tratamiento
* Una descripción sencilla de los fines del tratamiento
* La base jurídica del tratamiento
* Previsión o no de cesiones
* Referencia al ejercicio de derechos.

### 4.2.9. Derechos Schengen

El sistema de información Schengen (SIS) es un sistema de información a gran escala que facilita la cooperación entre las autoridades nacionales de control de aduanas, fronteras, y policía. Como complemento a este sistema, existe el sistema de información de visados (VIS), la normativa de este sistema reconoce el derecho al ejercicio de los derechos de acceso, rectificación y supresión, así como determinadas limitaciones a los mismos.

## 4.3. Deberes

El Reglamento General de Protección de Datos señala un conjunto de principios que los responsables y encargados del tratamiento deben observar al tratar datos personales:

* **Principio de “licitud, transparencia y lealtad”**, que consiste en que los datos deben ser tratados de manera licita, leal y transparente para el interesado.
* **Principio de “limitación de la finalidad”**, implica tanto la obligación de que los datos sean tratados con finalidades limitadas, y prohíbe que sean tratados con otros fines.
* **Principio de “minimización de datos”**, dice que los datos han de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
* **Principio de “exactitud”,** los datos han de ser exactos, y si es necesario, actualizarlos
* **Principio de “limitación del plazo de conservación”**. Relacionado con el de minimización. Una vez las finalidades para las que se han recabado los datos se han alcanzado, los datos han de ser borrados o desprovistos de todo elemento que permita identificar a los interesados.
* **Principio de “integridad y confidencialidad”**. Impone a quienes tratan los datos la obligación de actuar proactivamente con el objetivo de proteger los datos frente a cualquier amenaza a su seguridad.

### 4.3.1. Ejemplos de Medidas de Cumplimiento

En este apartado se verán diferentes medidas como ejemplos de este principio de responsabilidad.

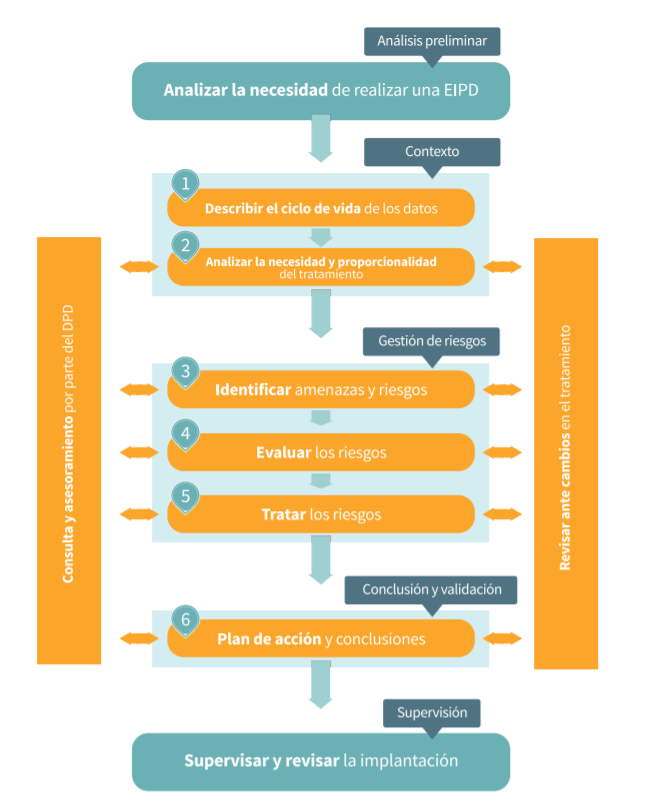
#### Brechas de seguridad

Una **brecha de seguridad** es un incidente de seguridad que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.

Según el reglamento Europeo 2016/679 General de protección de datos, en los artículos 33 y 34, se establece la obligación para las organizaciones de **notificar a la Autoridad de Control competente las brechas de seguridad** que puedan tener que ver con datos personales, y si estos daños son graves, **comunicar la brecha a las personas cuyos datos se hayan visto afectados** .Este plazo es de 72 horas desde que se conoce la brecha.

También hay que **notificar a la AEPD** y a los operadores de servicio de comunicaciones electrónicas disponibles al público.

#### Evaluaciones de Impacto (planes de contingencia)

Una **evaluación de impacto relativa a la Protección de Datos (EIPD)** describe, de manera anticipada y preventiva, un tratamiento de datos personales, evalúan la necesidad de la empresa de gestionar los potenciales riesgos a los que están expuestos dichos datos, y determinan las medidas necesarias para reducir estos riesgos hasta un nivel aceptable. La AEPD tiene una guía para realizar estos planes.

#### Transferencias internacionales

Los responsables de los datos podrán enviar estos a otros países sin necesidad de una autorización de la Agencia Española de Protección de Datos siempre que el tratamiento de datos cumpla lo dispuesto en el Reglamento General de Protección de Datos y se den los siguientes supuestos.

**Destinatario declarado adecuado por la Comisión Europea**

Los siguientes países están declarados de un nivel de protección adecuado, por lo que no hay problema en ceder los datos a un destinatario dentro de estos países. Los países son:

Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Estados Unidos y Japón.

**Sin declaración de adecuación, hacen falta garantías**

Las garantías son las siguientes:

* Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos
* Normativas corporativas vinculantes
* Cláusulas tipo de protección de datos adoptadas por la Comisión que siguen siendo válidas
* Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión
* Códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados
* Mecanismos de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados.

**En caso de que no haya declaración de adecuación, ni garantías:**

* El interesado ha dado su consentimiento
* La transferencia es necesaria para la ejecución de un contrato que incluye al interesado
* La transferencia es necesario por razones importantes de interés público
* La transferencia es necesaria para temas de reclamaciones
* La transferencia es necesaria para proteger los intereses vitales de del interesado u otras personas, y el interesado este incapacitado para dar su consentimiento.

**Se necesitará una autorización expresa de la AEPD cuando las garantías se aporten mediante:**

* cláusulas contractuales entre el responsable o el encargado y el responsable, y el encargado y sub encargado, que no hayan sido adoptadas por la Comisión Europea.
* disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

## 4.3. Donde y como actúa la AEPD

A continuación, veremos diferentes ámbitos donde actúa la AEPD, y ejemplos de como podemos ejercer nuestros derechos en cada uno de estos

### 4.3.1. Internet y redes Sociales

En internet siempre dejamos lo que se llama la **huella digital**, que es el rastro que dejamos mientras navegamos por la red. Los servicios mas usados de la red se nutren de esta huella digital para proveer servicios, tanto a empresas como a terceros.

**Derecho de supresión en buscadores de internet**

Anteriormente hemos hablado sobre lo que es el derecho de supresión. Los buscadores nos permiten ejercer este derecho si, por ejemplo salen resultados que no nos gustaría que se relacionaran con nuestro nombre, al buscar este en el buscador.

Este derecho lo podemos ejercer frente al buscador, pero tenemos que tener en cuenta que la información no se eliminará de su fuente digital, sino que este derecho al olvido solo afectará a las búsquedas hechas mediante el nombre de la persona.

Cada buscador tiene su propio formulario para eliminar la información, por ejemplo, [Google](https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637510821391004677-3336157358&hl=es&rd=1), [Bing](https://www.bing.com/webmaster/tools/eu-privacy-request) o [Yahoo!](https://es.ayuda.yahoo.com/kb/Solicitud-para-bloquear-resultados-de-b%C3%BAsqueda-en-Yahoo-Search-Recursos-para-Residentes-Europeos-sln28252.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYWVwZC5lcy8&guce_referrer_sig=AQAAACHy-_84-btdc8THBzYqCR6vJnLeBIG4ivDCpK8MH5_zKb0WFoghgNwg_xBpcECckqZXOx-91XxDmJVX7u9vJCMOEZXBByuaTr34HjZ8-8HZC28eMKkvpGwruO0EtE7ehOaJVkDqMBpVqOzAzBKE7oOtBPQy6dB6QMXxYZz8efOy).

**Eliminar fotos o vídeos de internet**

Las imágenes y los videos de una persona también son datos personales, por lo que su difusión sin tu consentimiento no está permitida.

El primer paso para eliminar un documento multimedia es hablar con la persona que lo subió, pero si esto no es posible, podemos contactar con la red social donde están subidos (Facebook, Google, Twitter, Instagram, TikTok, etc.) para que estas eliminen el contenido.

### 4.3.2. Publicidad no deseada

Si no deseas continuar recibiendo publicidad, puedes usar los siguientes métodos que nos propone la AEPD

**Inscribirse en una lista Robinson**

Las listas Robinson son listas cuya inscripción es gratuita, y que toda empresa que vaya a realizar una campaña publicitaria debe consultar, para excluir de dicha campaña a todo usuario que se haya dado de alta en una de estas listas. Sin embargo, podrán seguir enviándote publicidad si eres cliente de la empresa o has dado tu consentimiento explicito.

**Utilizando los medios provistos**

Muchas campañas de publicidad proveen medios para darse de baja de estas campañas. Por ejemplo, puedes mandar un correo electrónico a una dirección especifica para que no te llegue mas Spam de esa empresa, o un SMS a un numero para que te dejen de mandar publicidad al teléfono.

**Evitar dar tu consentimiento, o retirándolo**

En muchas ocasiones, basta con estar atento a la hora de participar en concursos o aprovechar ofertas, de no dar nuestros datos personales. Sin embargo, si ya es demasiado tarde para eso, siempre podrás revocar el consentimiento prestado.

**Desaparecer de las guías telefónicas**

También tienes derecho a no figurar en las guías telefónicas. Para ello, puedes dirigirte a la operadora con la que tienes contactada la línea y comunicarle que no deseas que tus datos personales sean publicados en las guías de abonados.

**Sistema de mediación**

La Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL) ha diseñado un sistema de mediación para obtener una respuesta ágil en reclamaciones que puedan afectar al tratamiento de datos de carácter personal de los ciudadanos, como puede ser la recepción de publicidad no deseada.

### 4.3.3. Violencia de género y violencia digital

La AEPD colabora con la Delegación del Gobierno contra la Violencia de Genero y el Ministerio de Igualdad para brindar apoyo a las mujeres victimas de este delito, ya que en su caso, sus niveles de privacidad, en especial de los dispositivos móviles, pueden ser una cuestión de vida o muerte.

### 4.3.4. Protección de datos y Coronavirus

Ante la situación de emergencia de salud pública derivada de la extensión del coronavirus, la Agencia Española de Protección de Datos ha elaborado varios recursos en relación con el COVID-19 para dar respuesta a las dudas que han ido surgiendo en estos días. Estos recursos van desde informes sobre el tratamiento de datos, hasta notas de prensa, pasando por una sección de preguntas frecuentes.

Puedes consultar todos estos recursos [en este enlace](https://www.aepd.es/es/areas-de-actuacion/proteccion-datos-y-coronavirus).

### 4.3.5. Educación y menores

La AEPD ha desarrollado una pagina web llamada [tudecideseninternet.net](https://www.tudecideseninternet.es/aepd/), cuya finalidad es brindar ayuda a los jóvenes con la protección de datos, así como educarlos en este tema para que se encuentren con la menor cantidad de problemas posibles con guías y videos didácticos.

### 4.3.6. Videovigilancia

La AEPD tiene a disposición publica numerosos ficheros con requisitos para cumplir la normativa de protección de datos en videovigilancia. A continuación analizaremos, por ejemplo, su uso en una comunidad de propietarios.

Primero, para la instalación de cámaras, se debe haber aprobado en junta de Propietarios. A la hora de colocarlas, se debe ejercer el derecho de información, colocando carteles que informan que se accede a una zona videovigilada. A la hora de la instalación, las cámaras solo podrán captar imágenes de las zonas comunes de la comunidad, nunca de la via publica, salvo que resulte necesario para la finalidad perseguida. El acceso a las imágenes esta restringido a las personas designadas por la comunidad. Las imágenes se conservaran como máximo un mes.

## 4.4. Herramientas que proporciona la AEPD

La AEPD facilita diversas herramientas, con diferentes finalidades, para ayudar a cumplir todo lo que estipula relacionado con la protección de datos.

### 4.4.1. Facilita RGPD

Es una herramienta de ayuda para empresas que realicen un tratamiento de datos personales de escaso riesgo para el cumplimiento del Reglamento General de Protección de Datos.

Es una herramienta fácil y gratuita, que con solo tres pantallas de preguntas muy concretas permite a quien la utiliza valorar su situación respecto del tratamiento de datos personales que lleva a cabo: si se adapta a los requisitos exigidos para utilizar Facilita RGPD o si debe realizar un análisis de riesgos.

### 4.4.2. Canal del Delegado de Protección de Datos

El canal del Delegado de Protección de Datos (DPD) tiene como finalidad atender las consultas planteadas ante la AEPD por los Delegados de Protección de Datos, tanto del sector público como del privado, al desempeñar las funciones encomendadas en el artículo 39 del Reglamento General de Protección de datos (RGPD).

### 4.4.3. Gestiona EIPD

Es un asistente para el análisis de riesgos y evaluaciones de impacto en protección de datos. Esta herramienta gratuita guía a los responsables y encargados del tratamiento en los aspectos que se deben tener en cuenta, proporcionando una base inicial para una gestión adecuada.

En general, es una herramienta de ayuda y soporte a la decisión, y cuya utilización genera la documentación básica sobre la cual hay que realizar un análisis y gestión del riesgo por parte de responsables y encargados para cumplir con lo previsto en el reglamento general de protección de datos y la LOPDGDD.

### 4.4.4. Facilita Emprende

Esta nueva herramienta persigue servir de apoyo a emprendedores y startups cuyos tratamientos se caracterizan por un fuerte componente innovador que hace uso de nuevas tecnologías.

Su uso es similar a Facilita-RGPD, teniendo unos cuestionarios, y al finalizarlos se da un conjunto de documentos adaptados como guía y apoyo para cumplir con las obligaciones de protección de datos.

### 4.4.5. Comunica-Brecha RGPD

Esta herramienta es un recurso para que cualquier organización, responsable de un tratamiento de datos personales, pueda valorar la obligación de informar a las personas físicas afectadas por una brecha de seguridad de los datos personales, tal y como establece el artículo 34 del Reglamento General de Protección de Datos.

# 5. Ejemplos de sentencias

En este apartado, leeremos algunas sentencias relacionadas con la protección de datos, y las comentaremos de acuerdo con lo aprendido a lo largo del trabajo

## 5.1. Multa a la Mutua Madrileña (Procedimiento nº.: PS/00586/2017)–