

# Tema 5: Protección de datos personales

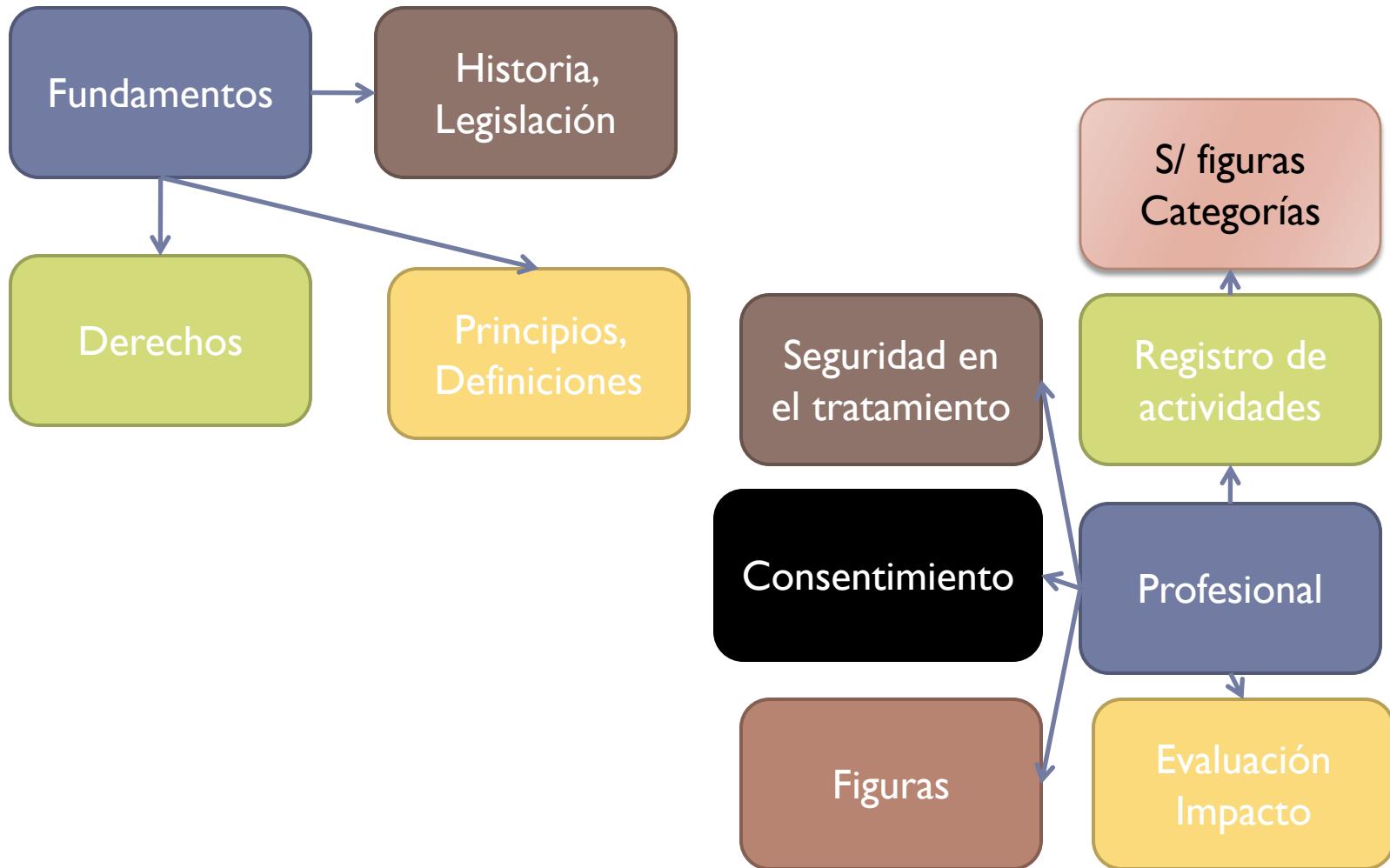
---

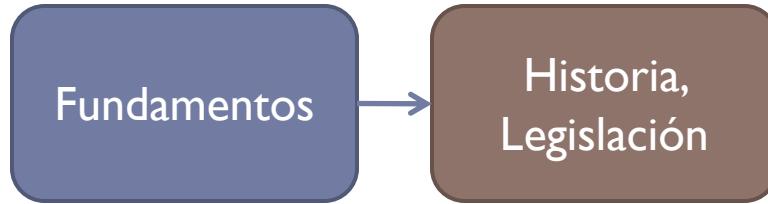
Juan V. Oltra

Errare humanum est perseverare diabolicum. *Lucius Annaeus Seneca*

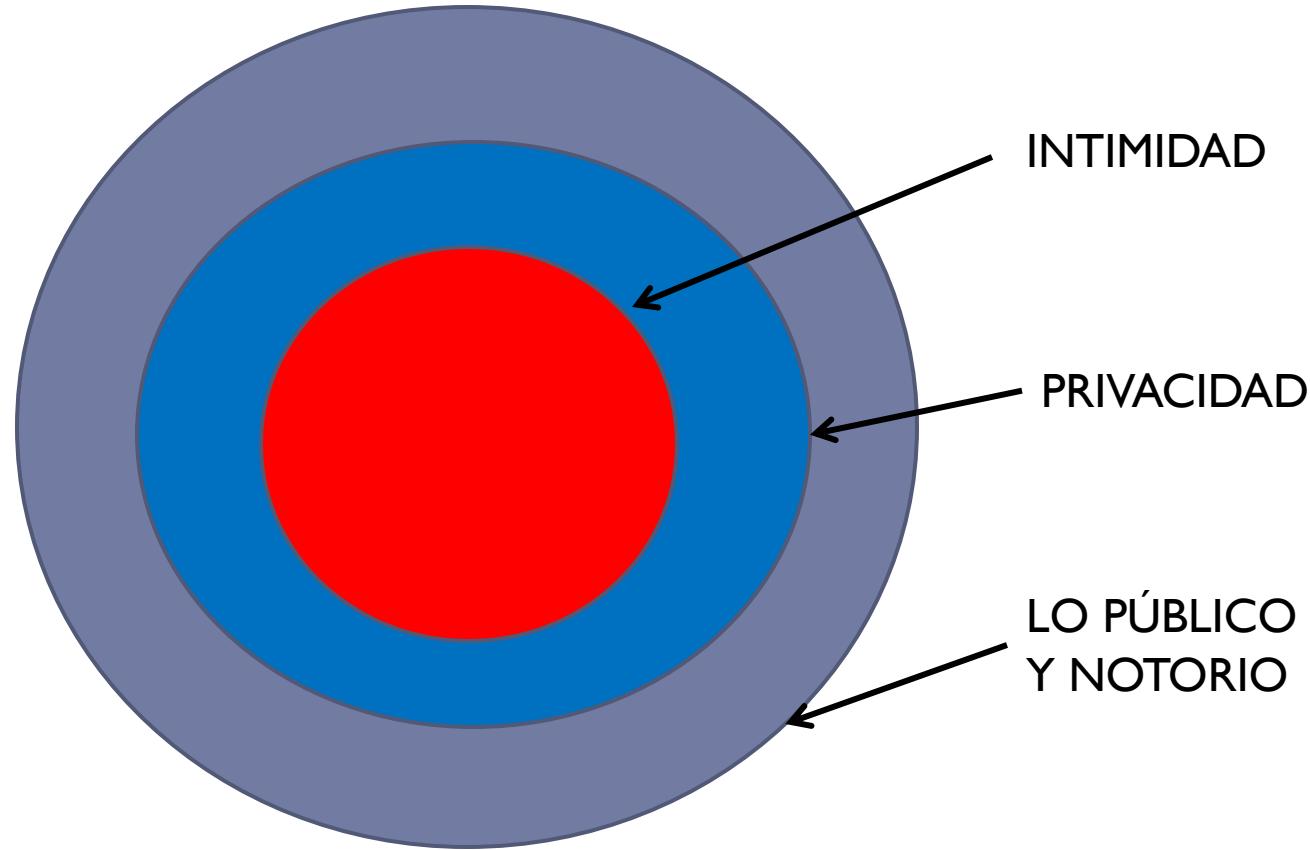
# Índice

- ▶ **Introducción**
  - ▶ Historia
- ▶ **Figuras**
  - ▶ Responsable, Encargado, DPD
- ▶ **Definiciones y principios**
- ▶ **Derechos**
- ▶ **Agencia de Protección de Datos**
- ▶ **Trabajos del profesional**
- ▶ **Particularidades**
  - ▶ Datos singulares, transferencias...
- ▶ **Sanciones**
- ▶ **Derechos digitales**
- ▶ **Ética**





# ¿Qué es la privacidad?

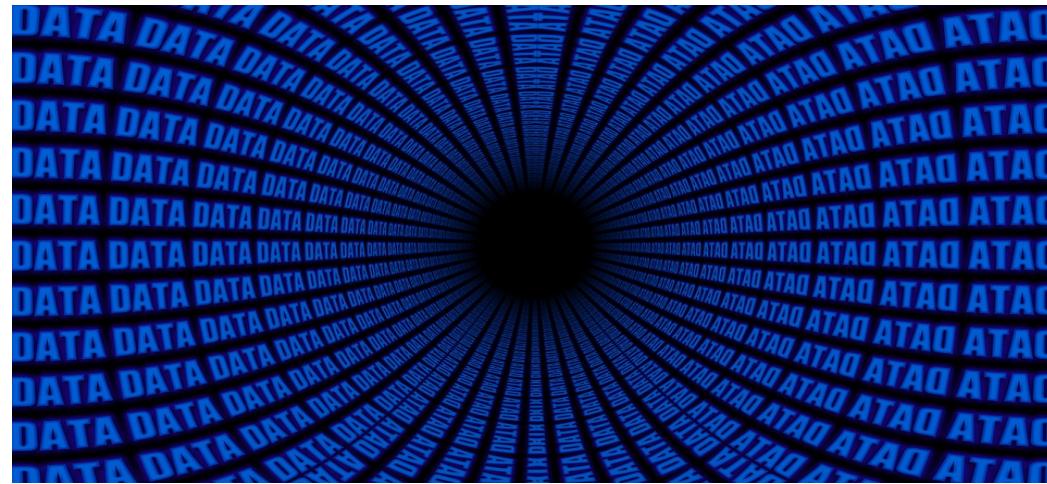


# Marco: ¿Qué es eso de “protección de datos”?

- ▶ Es un derecho fundamental ....
- ▶ Es una disciplina jurídica...
- ▶ Es una Ley Orgánica...
- ▶ Es...
- ▶ Es algo que siempre, de alguna manera ha estado aquí

Grecia

Roma



E. Media

E. Moderna

S. Información

# Derecho fundamental... disciplina jurídica...

- ▶ ¿Es un derecho fundamental?. El Tribunal Constitucional (sentencia TC 292/2000) dice que sí (véase).
- ▶ Como disciplina jurídica busca proteger la intimidad y demás derechos fundamentales de las personas físicas frente al riesgo que supone la recopilación y el uso indiscriminado de sus datos personales,
  - ▶ Abarca todo tipo de tratamiento (independientemente de que se realice de manera manual o informatizada)
  - ▶ Necesidad de desarrollar normas que limitando el uso de los datos personales, garanticen el honor y la intimidad personal y familiar de los ciudadanos.



# Historia...

## HARVARD LAW REVIEW.

VOL. IV.

DECEMBER 15, 1890.

NO. 5.

THE RIGHT TO PRIVACY.

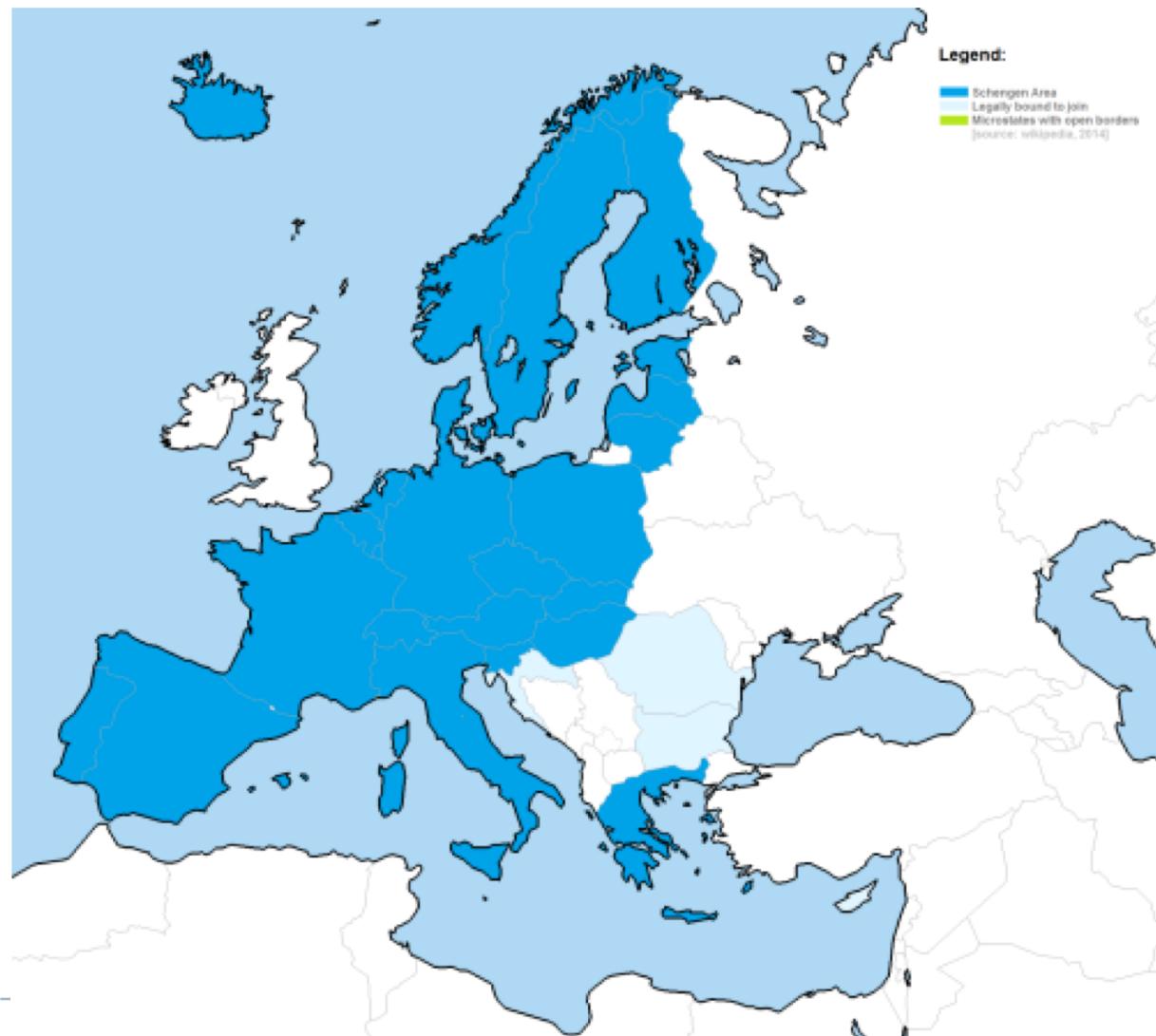
1967												
ENERO					FEBRERO					MARZO		
L	M	M	J	V	S	D	L	M	M	J	V	S
•	•	•	•	•	1		•	•	1	2	3	4
2	3	4	5	6	7	8	6	7	8	9	10	11
9	10	11	12	13	14	15	13	14	15	16	17	18
16	17	18	19	20	21	22	20	21	22	23	24	25
23	24	25	26	27	28	29	27	28	•	•	•	•
30	31						27	28	29	30	31	•
ABRIL					MAYO					JUNIO		
L	M	M	J	V	S	D	L	M	M	J	V	S
•	•	•	•	1	2		1	2	3	4	5	6
3	4	5	6	7	8	9	8	9	10	11	12	13
10	11	12	13	14	15	16	15	16	17	18	19	20
17	18	19	20	21	22	23	22	23	24	25	26	27
24	25	26	27	28	29	30	29	30	31	•	•	•
JULIO					AGOSTO					SEPTIEMBRE		
L	M	M	J	V	S	D	L	M	M	J	V	S
•	•	•	•	1	2		•	1	2	3	4	5
3	4	5	6	7	8	9	7	8	9	10	11	12
10	11	12	13	14	15	16	14	15	16	17	18	19
17	18	19	20	21	22	23	21	22	23	24	25	26
24	25	26	27	28	29	30	28	29	30	31	•	•
OCTUBRE					NOVIEMBRE					DICIEMBRE		
L	M	M	J	V	S	D	L	M	M	J	V	S
•	•	•	•	1			•	1	2	3	4	5
2	3	4	5	6	7	8	6	7	8	9	10	11
9	10	11	12	13	14	15	13	14	15	16	17	18
16	17	18	19	20	21	22	20	21	22	23	24	25
23	24	25	26	27	28	29	27	28	29	30	•	•
30	31						25	26	27	28	29	30

# LOPD: Un poco de historia



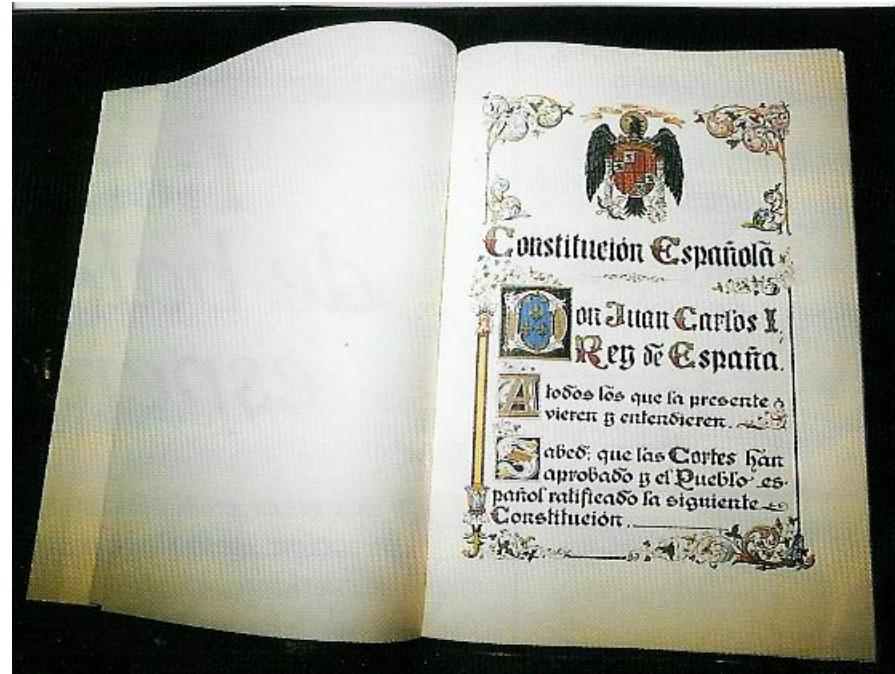
- ▶ MY 67: Conferencia de Juristas Nómicos.
  - ▶ protección de la vida privada (nuevas formas de injerencia)
- ▶ Comisión consultiva del Consejo de Europa
  - ▶ para estudiar TIC y su influencia sobre los derechos de la persona: Resolución 68/509/CE de la Asamblea del Consejo de Europa, sobre "los derechos humanos y los nuevos logros científicos y técnicos"
- ▶ 19 dic 68 ONU: Resol 2450 (XXIII)
  - ▶ necesidad de fijar límites a las aplicaciones de la electrónica.
- ▶ 1970, resol 428 de la Asamblea Consultiva del Consejo de Europa: "intimidad como un objeto de obligada protección frente a la intromisión de la tecnología de la información"
- ▶ 1967: A.C. del C. de E.: 1973 resol (73) 22 de 26 de septiembre: "protección de la vida privada de las personas físicas frente al sector privado". 74 (29): idem s/ sector público.
- ▶ 1980, 28 sept. Consejo de Ministros del Consejo de Europa: convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal.
- ▶ (Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa de 1981)

# De especial importancia: espacio Schengen



# Piedra basal...

- ▶ Artículo 18 C.E.
- ▶ 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.



# Antecedentes

## ▶ Antecedentes

- ▶ LO 1/1982, 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen
- ▶ LORTAD, Ley Orgánica 5/1992, de 29 de octubre
- ▶ RD 1332/1994, desarrollo aspectos de la LORTAD
- ▶ RD 994/1999, Reglamento LORTAD
- ▶ Directiva Comunitaria 95/46/CE de 24/octubre/95, que exigía extensión a ficheros manuales.
- ▶ Ley Orgánica 15/1999, de 13 de diciembre, LOPD
- ▶ RD 1720/2007, Reglamento de la LOPD.
- ▶ RGPD



## LEGISLACIÓN CONSOLIDADA

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

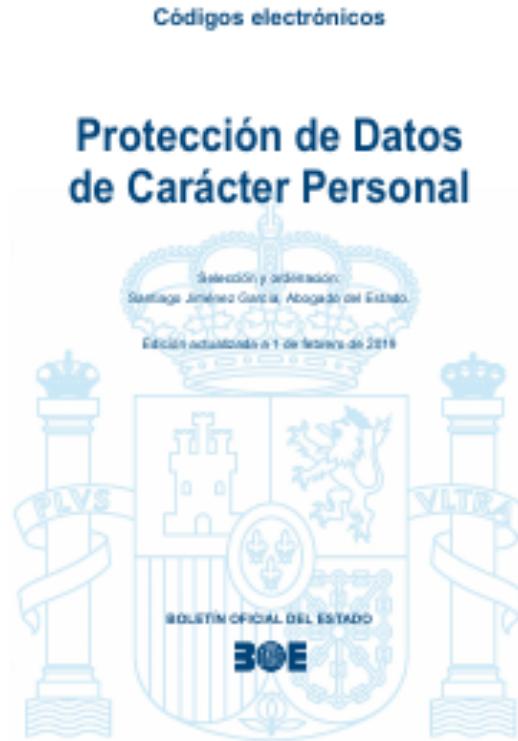
Jefatura del Estado  
«BOE» núm. 294, de 6 de diciembre de 2018  
Referencia: BOE-A-2018-16673

# Otras normas



- ▶ 12/1989 Reguladora de la función estadística pública
- ▶ 16/1985 de Patrimonio histórico español
- ▶ 13/1986 de Fomento y coordinación general de la investigación científica y técnica
- ▶ 3/2003 Ley de telecomunicación
- ▶ 34/2002 LSSI
- ▶ 56/2007 de Medidas de Impulso de la Sociedad de la Información.
- ▶ 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (lucha terrorismo y crimen organizado)

¿Mucho lío? BOE.es → Legislación / códigos



- ▶ I de febrero de 2019 | 4 de enero de 2019
  - ▶ Aprox. 500 pgs.                    Aprox. 1000 pgs.

# Marco básico

## REGLAMENTOS

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 27 de abril de 2016

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales  
y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento  
general de protección de datos)

(Texto pertinente a efectos del EEE)



## LEGISLACIÓN CONSOLIDADA

Ley Orgánica 3/2018, de 5 de diciembre, de  
Protección de Datos Personales y garantía de  
los derechos digitales.

Jefatura del Estado  
«BOE» núm. 294, de 6 de diciembre de 2018  
Referencia: BOE-A-2018-16673

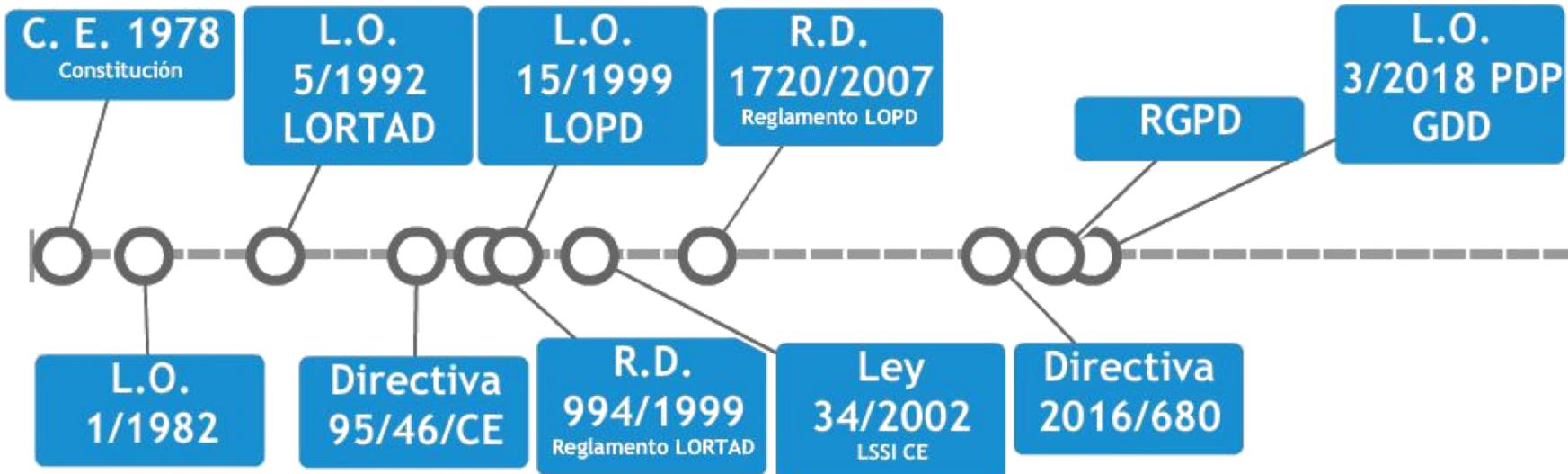
# Otros: legislación autonómica

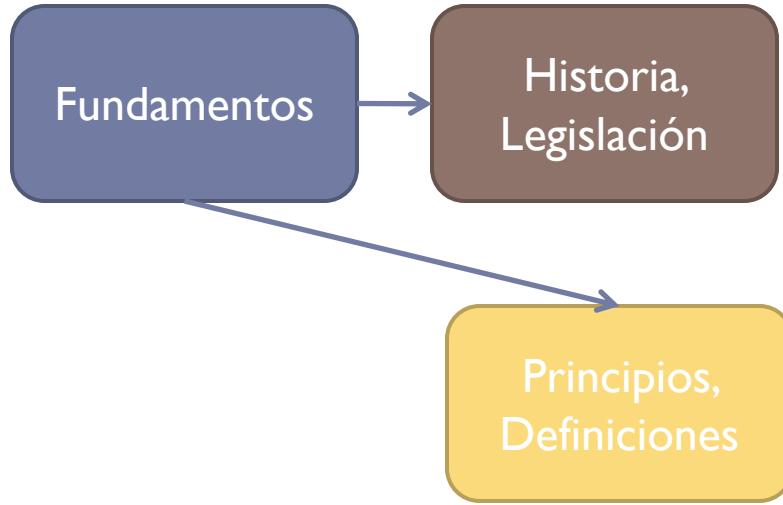
## ▶ Destacamos por su interés:

- ▶ Ley 5/2002 (Comunidad Autónoma de Cataluña), de 19 de abril, de la Agencia Catalana de protección de datos.
- ▶ Ley 8/2001 (Comunidad Autónoma de Madrid), de 13 de julio, de protección de datos de carácter personal en la Comunidad de Madrid.
- ▶ Pero... ¡hay más! ¡mucha más!
  - ▶ (Galicia -uso y acceso a la historia
  - ▶ clínica electrónica- y País Vasco)
  - ▶ Para empezar... ver [aquí](#).



# Línea de tiempo con los elementos principales



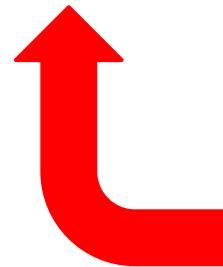


# Principios – la calidad de los datos

- ▶ Licitud, **lealtad** y transparencia
- ▶ Limitación de la **finalidad**
- ▶ Minimización de datos: adecuados, **pertinentes** y limitados a lo necesario en relación con los fines para los que son tratados
- ▶ **Exactitud**: exactos y actualizados
- ▶ Integridad y confidencialidad: se garantiza una **seguridad** adecuada de los datos personales
- ▶ **ADECUADOS + PERTINENTES + NO EXCESIVOS = CALIDAD**

# Datos personales

- ▶ toda información sobre una **persona física** identificada o identifiable («el interesado»); se considerará persona física identifiable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;



REGLAMENTOS

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

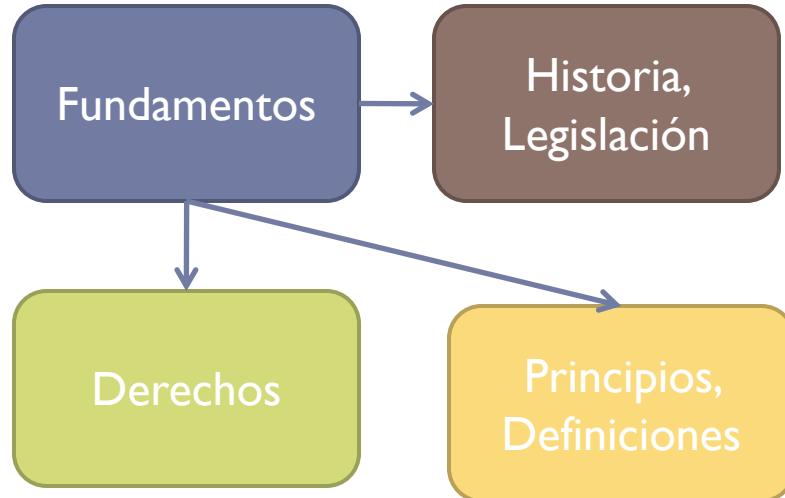
de 27 de abril de 2016

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

(Texto pertinente a efectos del EEE)

# Ejemplos

Datos aislados no afectados	Datos afectados
1979	Alberto Martínez Pujol
46071	<a href="http://www.pepemaiquez.net">http://www.pepemaiquez.net</a>
95%	158.153.205.26
Barcelona	C\ Pato Cojo, 23, pta. 18
Amarillo	jacinto.quincoces@gmail.com



# Derechos (ciudadano vs responsable del tratamiento)

- ▶ Acceso
- ▶ Rectificación
- ▶ Supresión (olvido)
- ▶ Limitación del tratamiento
- ▶ Portabilidad
- ▶ Oposición



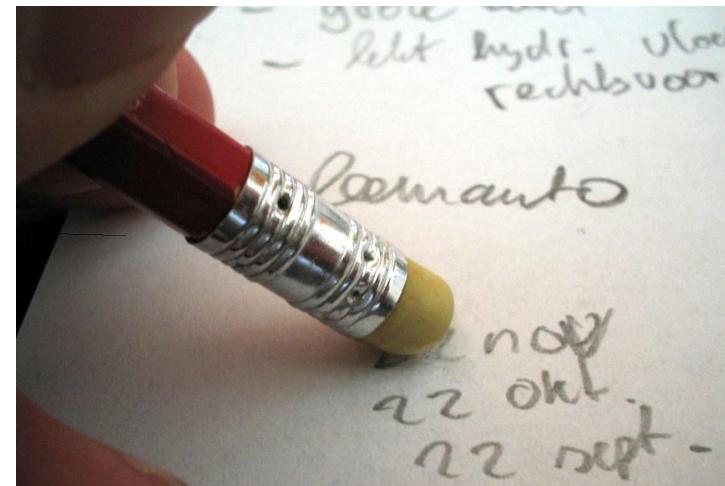
# Acceso

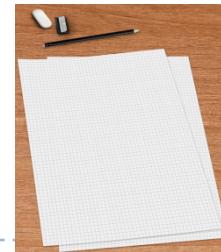


- ▶ Confirmación de si se están tratando o no datos personales que le conciernen
  - ▶ fines del tratamiento;
  - ▶ categorías de datos personales de que se trate;
  - ▶ destinatarios (en particular terceros u organizaciones internacionales)
  - ▶ plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinarlo
  - ▶ existencia del derecho a solicitar rectificación, supresión, limitación del tratamiento u oposición, y del derecho a presentar una reclamación ante una autoridad de control
  - ▶ Si no se han obtenido del interesado, cualquier información disponible sobre su origen y la existencia de decisiones automatizadas (perfiles).

# Rectificación

- ▶ Obtener sin dilación la rectificación de los datos personales inexactos que le conciernan.
- ▶ Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

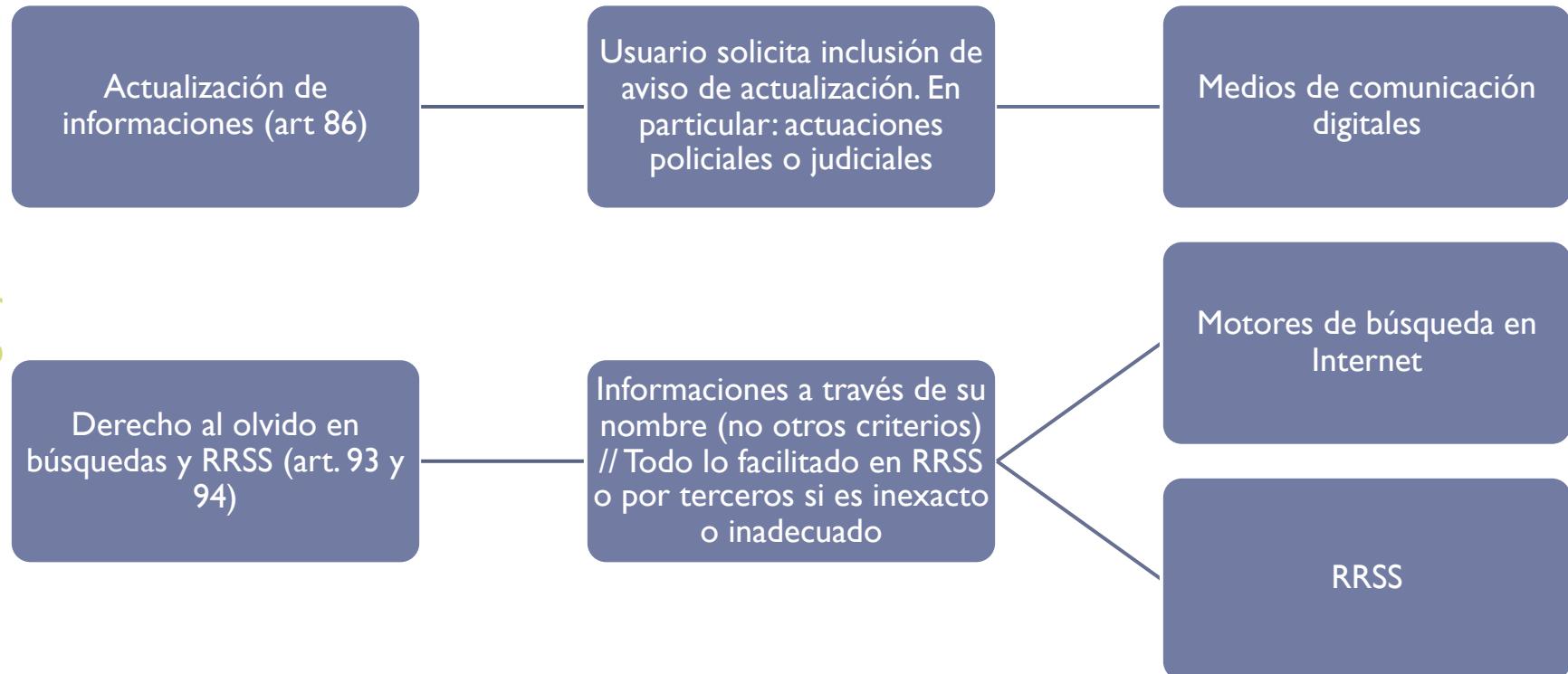




# Supresión (derecho al olvido)

- ▶ Supresión de los datos personales que le conciernan, sin dilación indebida cuando:
  - ▶ los datos personales **ya no sean necesarios** en relación con los fines para los que fueron recogidos o tratados de otro modo;
  - ▶ el interesado **retire el consentimiento**
  - ▶ el interesado se oponga al tratamiento y no prevalezcan otros motivos;
  - ▶ los datos personales hayan sido tratados ilícitamente;
  - ▶ deban suprimirse para el cumplimiento de una obligación legal
  - ▶ se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1. (**menores**)
- ▶ **Si se han hecho públicos y esté obligado a suprimirlos**, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

# Actualización de informaciones / Derecho al olvido





# Limitación del tratamiento

- ▶ Limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:
  - ▶ el interesado **impugne la exactitud** de los datos personales, durante un plazo que permita al **responsable verificar** la exactitud de los mismos;
  - ▶ el **tratamiento sea ilícito** y el **interesado se oponga** a la **supresión** de los datos personales y solicite en su lugar la limitación de su uso;
  - ▶ el responsable ya no necesite los datos personales para los fines del tratamiento, pero el **interesado los necesite** para la formulación, el ejercicio o la defensa de **reclamaciones**;
  - ▶ el **interesado se haya opuesto al tratamiento**, mientras se **verifica si los motivos legítimos** del responsable prevalecen sobre los del interesado.

# Portabilidad

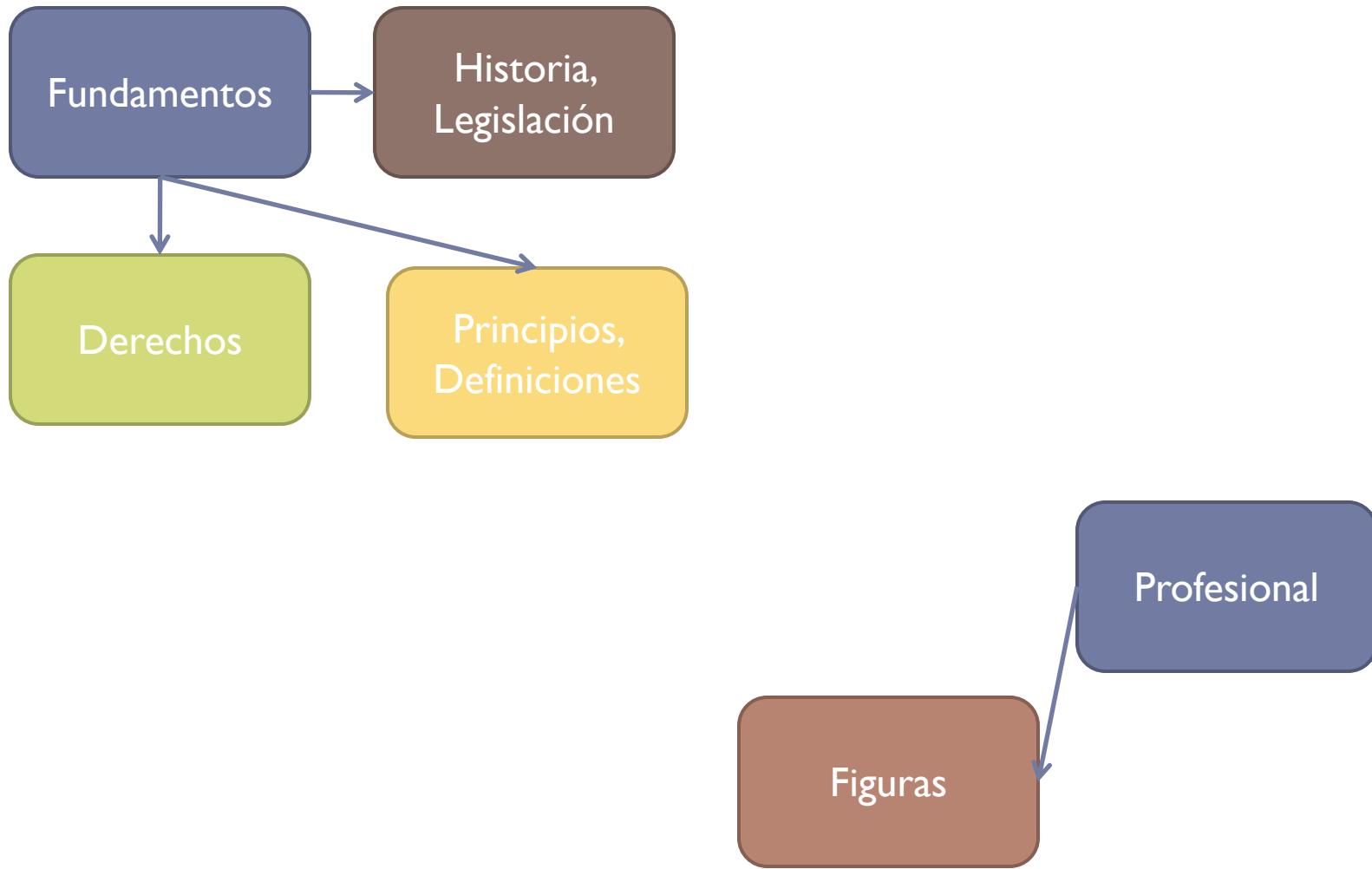


- ▶ El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: el tratamiento esté basado en el consentimiento o en un contrato y el tratamiento se efectúe por medios automatizados.
- ▶ El interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.



# Oposición

- ▶ Oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento incluida la elaboración de perfiles sobre la base de dichas disposiciones.
- ▶ Salvo que se acrediten motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.
- ▶ Cuando el tratamiento tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento, incluida la elaboración de perfiles.



# Figuras clave

- ▶ Responsable
- ▶ Encargado
- ▶ Delegado de protección de datos (DPD)





# Responsable vs Encargado vs...

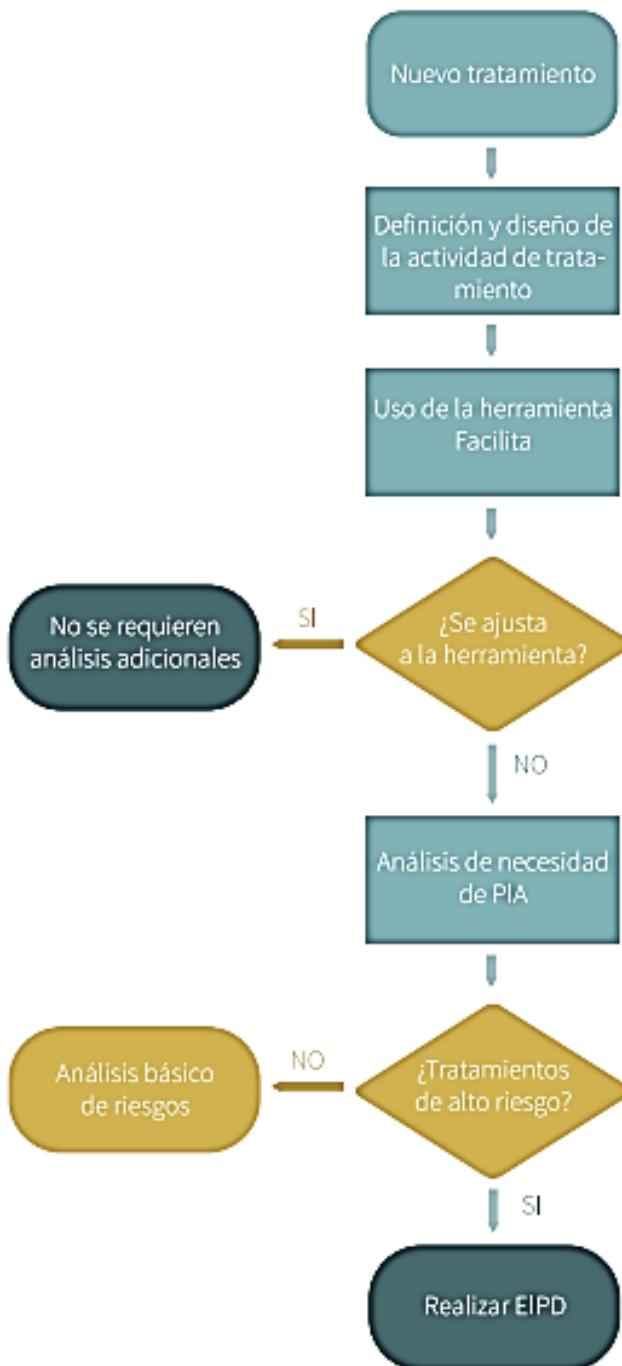
- ▶ Responsable: la persona física o jurídica, autoridad pública, servicio u otro organismo que, **solo o junto con otros, determine los fines y medios del tratamiento;**
- ▶ Encargado: la persona física o jurídica, autoridad pública, servicio u otro organismo **que trate datos personales por cuenta del responsable del tratamiento;**
- ▶ Destinatario: a quien se comuniquen datos personales, se trate o no de un tercero. **(No autoridades en el marco de una investigación)**
  - ▶ Tercero: alguien distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado



# El profesional, el encargado...



- ▶ Debe preguntarse
  - ▶ ¿se pueden generar con el tratamiento situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño... ?
  - ▶ ¿se puede privar a los afectados de sus derechos y libertades?
  - ▶ ¿Se trabaja con categorías especiales de datos o datos relacionados con la comisión de infracciones administrativas?
    - ▶ Datos genéticos
    - ▶ Datos biométricos
    - ▶ Datos relativos a la salud...
  - ▶ ¿Se crean perfiles? ¿sobre economía, salud...?
  - ▶ ¿Se trata de datos de grupos de afectados vulnerables?
    - ▶ menores de edad y personas con discapacidad
  - ▶ ¿Se trata de un tratamiento masivo?
  - ▶ ¿Va a darse una transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales sin un nivel adecuado de protección?
- ▶ Debe considerar: códigos de conducta y estándares definidos.



ción de datos personales



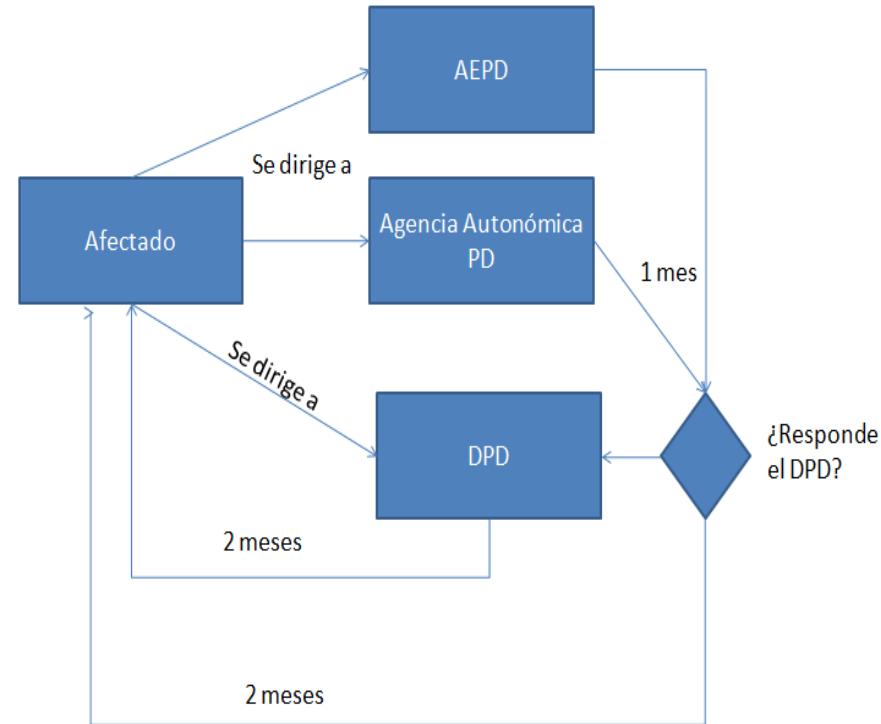
# Delegado de Protección de Datos (DPD)



- ▶ ¿Qué es?... un **especialista en derecho de protección de datos**, con unas funciones que le hacen parecer una suerte de defensor del pueblo de los datos.
  - ▶ **Informar y asesorar a los responsables y encargados** del tratamiento de datos personales (y a sus empleados) de las obligaciones que tienen, derivadas tanto de la legislación.
  - ▶ **Supervisar el cumplimiento de la legislación** y de la política interna de protección de datos de una Administración Pública o empresa.
  - ▶ Cuando se le solicite, **asesorar sobre la evaluación de impacto** de un tratamiento de datos personales (sobre este interesante elemento volveremos), cuando entrañe un alto riesgo para los derechos y libertades de las personas físicas, y supervisar luego su aplicación.
  - ▶ **Cooperar con las “autoridades de control”** (esto es, con las Agencias de Protección de Datos)
  - ▶ **Servir de ventanilla o punto de contacto** de las autoridades de control para cualquier consulta sobre el tratamiento de datos personales.

# DPD: interlocutor necesario

- ▶ ¿El DPD debe estar certificado por alguna entidad? ¿Puede no ser una persona?
  - ▶ No es obligatorio certificarse y no debe ser por obligación una persona física. Pero pasar por los procesos voluntarios de certificación es muy ventajoso.
- ▶ El DPD será **el interlocutor con la Agencia**, no podrá ser despedido ni sancionado, salvo que incurra en dolo o negligencia grave y no se le puede negar el acceso a los datos



# Trabajos más relevantes del profesional

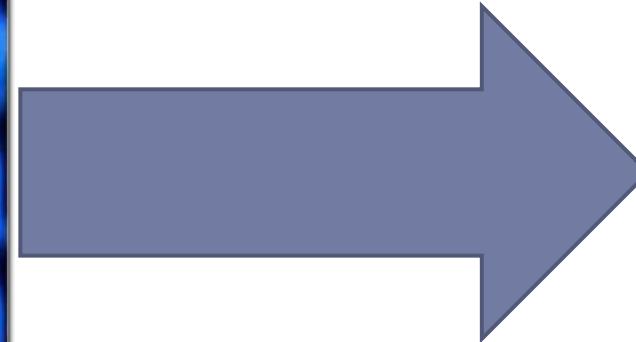
- ▶ Registro de actividades
- ▶ Seguridad del tratamiento
- ▶ Evaluación del impacto
- ▶ Consentimiento



# ¿Qué implica la responsabilidad activa recogida en el Reglamento?

- ▶ Las empresas deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías:
  - ▶ Protección de datos **desde el diseño**
  - ▶ Protección de datos **por defecto**
  - ▶ Medidas de seguridad
  - ▶ Mantenimiento de **un registro de tratamientos**
  - ▶ Realización de **evaluaciones de impacto** sobre la protección de datos
  - ▶ Nombramiento de un delegado de protección de datos
  - ▶ **Notificación de violaciones de la seguridad** de los datos
  - ▶ Promoción de **códigos de conducta** y esquemas de certificación.

# ¿Consejos para cumplir la normativa?

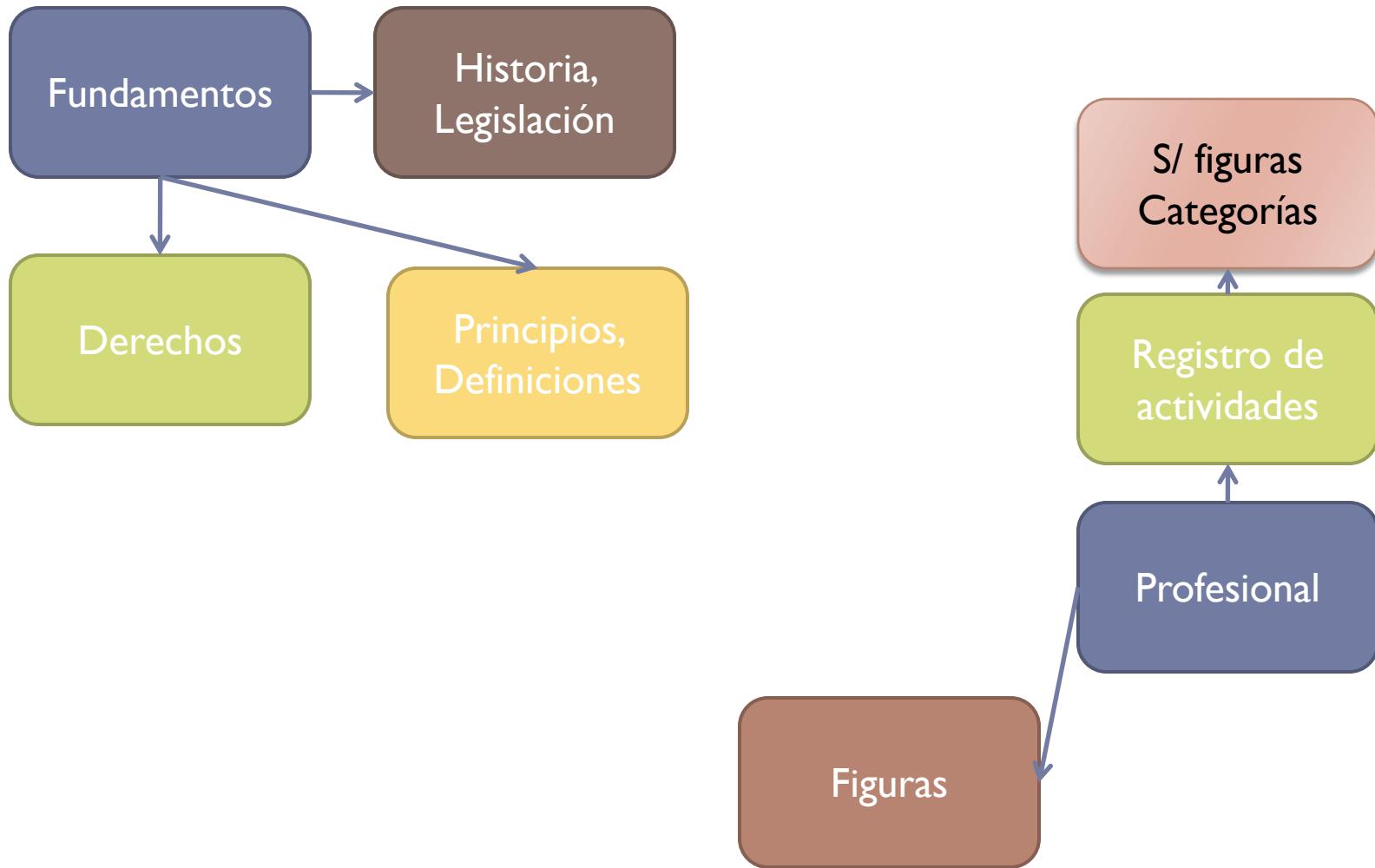


## Listado

# Empresa: Riesgos y obligaciones

- ▶ Régimen sancionador: a criterio de órganos reguladores
- ▶ ANÁLISIS DE RIESGOS.
  - ▶ Ante el contrato
  - ▶ Evaluación de Impacto.
- ▶ OBLIGACIONES:
  - ▶ Registro de actividad
  - ▶ Garantizar la seguridad de los datos tratados
  - ▶ Cooperación con la autoridad de control
  - ▶ Notificar violaciones de seguridad
  - ▶ Designar un delegado de PPDD





# Registro de actividades



- ▶ Cada **responsable** llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Debe contener:
  - ▶ Nombre y los datos de contacto del responsable (y corresponsable), del representante del responsable, y del delegado de protección de datos;
  - ▶ **los fines del tratamiento;**
  - ▶ Descripción de las categorías de interesados y de las categorías de datos personales;
  - ▶ Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales;
  - ▶ Si se dan, las transferencias de datos personales a un tercer país;
  - ▶ Cuando sea posible:
    - ▶ **plazos previstos** para la supresión de las diferentes categorías de datos;
    - ▶ descripción general de las medidas técnicas y organizativas de seguridad.



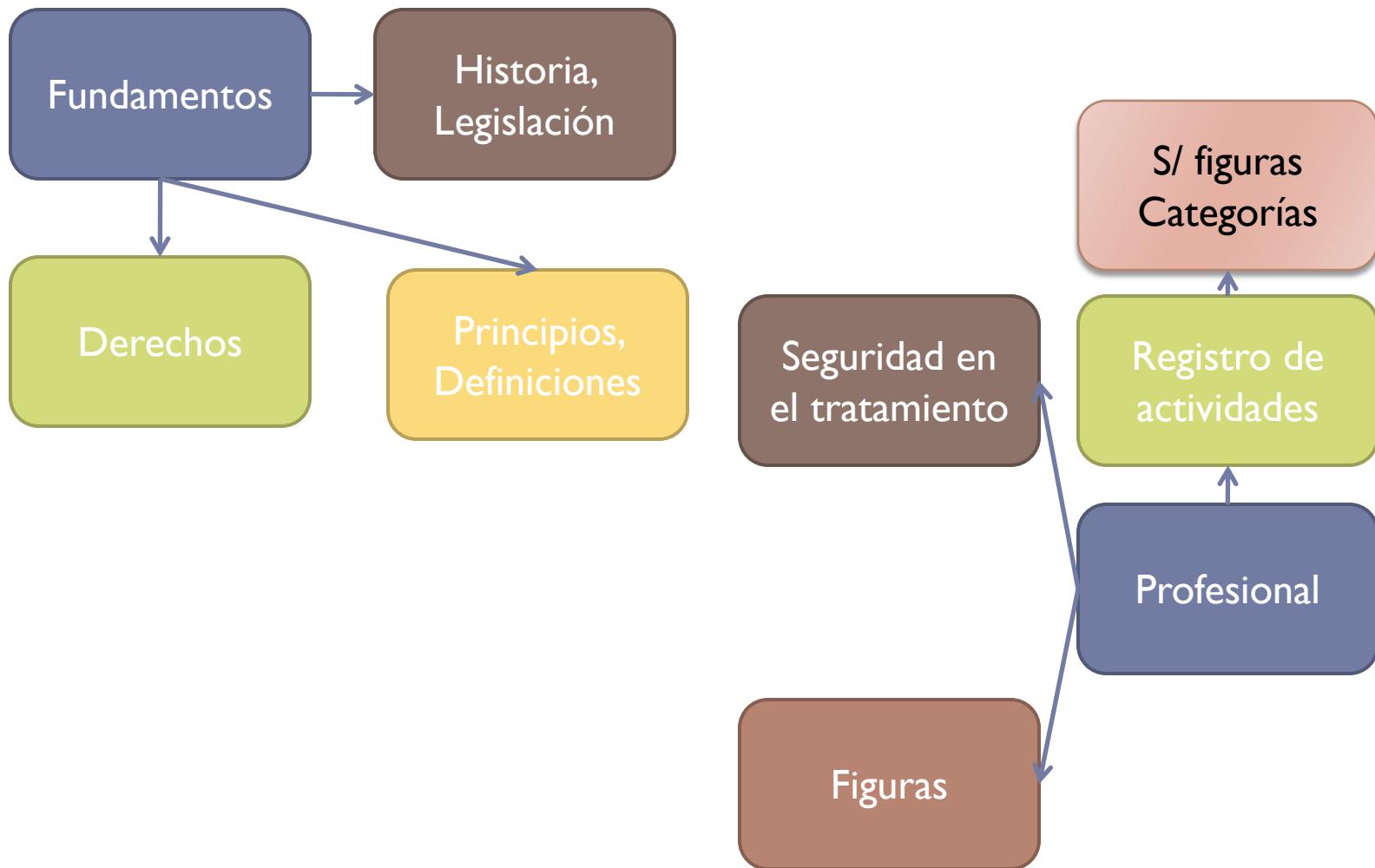
# Registro de actividades - encargado

- ▶ Cada encargado:
  - ▶ un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable
    - ▶ Nombre y los datos de contacto del encargado o encargados, responsables y delegado de protección de datos;
    - ▶ Categorías de tratamientos efectuados por cuenta de cada responsable;
    - ▶ Si se dan, transferencias de datos personales a un tercer país;
    - ▶ Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.
- ▶ Los registros, de encargado y responsable:
  - ▶ por escrito
  - ▶ a disposición de la autoridad de control que lo solicite.
  - ▶ **NO SON aplicables a empresas de menos de 250 personas,**
    - ▶ Excepto si el tratamiento que realice pueda entrañar un riesgo o incluya categorías especiales de datos personales.

# Categorías de tratamiento

- ▶ **ALTO RIESGO**
  - ▶ Tratamiento con alto riesgo
- ▶ **INTERNACIONAL**
  - ▶ Transferencias internacionales de datos
- ▶ **PERFILES**
  - ▶ Elaboración de perfiles
- ▶ **GRUPO**
  - ▶ Datos tratados por grupos de empresas
- ▶ **PÚBLICO**
  - ▶ Datos de titularidad o interés público

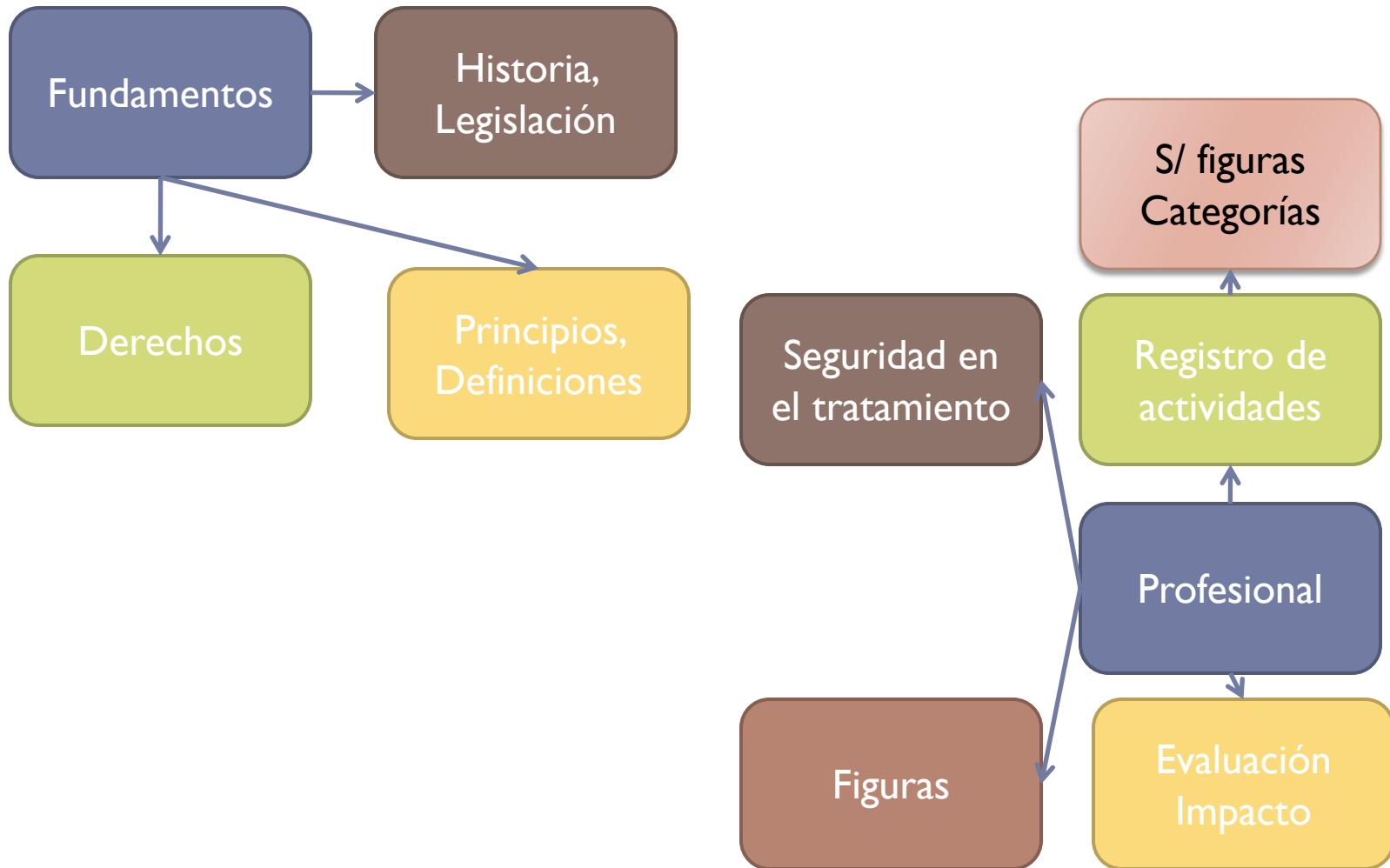






# Seguridad del tratamiento

- ▶ Considerando el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
  - ▶ seudonimización y el cifrado de datos personales;
  - ▶ capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
  - ▶ la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
  - ▶ proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
- ▶ Riesgos más preocupantes serían la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados.
- ▶ Protección de datos desde el diseño y por defecto: art 25





# Evaluación del impacto

- ▶ Evaluar de **manera anticipada** cuáles son los potenciales **riesgos** a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos.
- ▶ El análisis de riesgos permite identificar los riesgos que se ciernen sobre los datos de los interesados y **establecer una respuesta** adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.
- ▶ El RGPD prevé que las Evaluaciones de Impacto se lleven a cabo “**antes del tratamiento**”

<https://gestiona.aepd.es/>

## GESTIONA EIPD

La Evaluación de Impacto en la Protección de Datos Personales (EIPD) es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

La EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

El resultado de la EIPD se debe tener en cuenta, necesariamente, a la hora de tomar las decisiones relacionadas con el cumplimiento de lo previsto en el RGPD y la toma de decisión de la viabilidad o no de llevar a cabo el tratamiento de los datos.

Una EIPD no se requiere siempre, en cada actividad de tratamiento, se debe valorar la necesidad de llevar a cabo la misma. Es fundamental realizar el siguiente análisis previo para determinar de forma preliminar el nivel de riesgo al que puede estar expuesto el tratamiento y tomar la decisión adecuada en base a ello.

Herramienta FACILITA



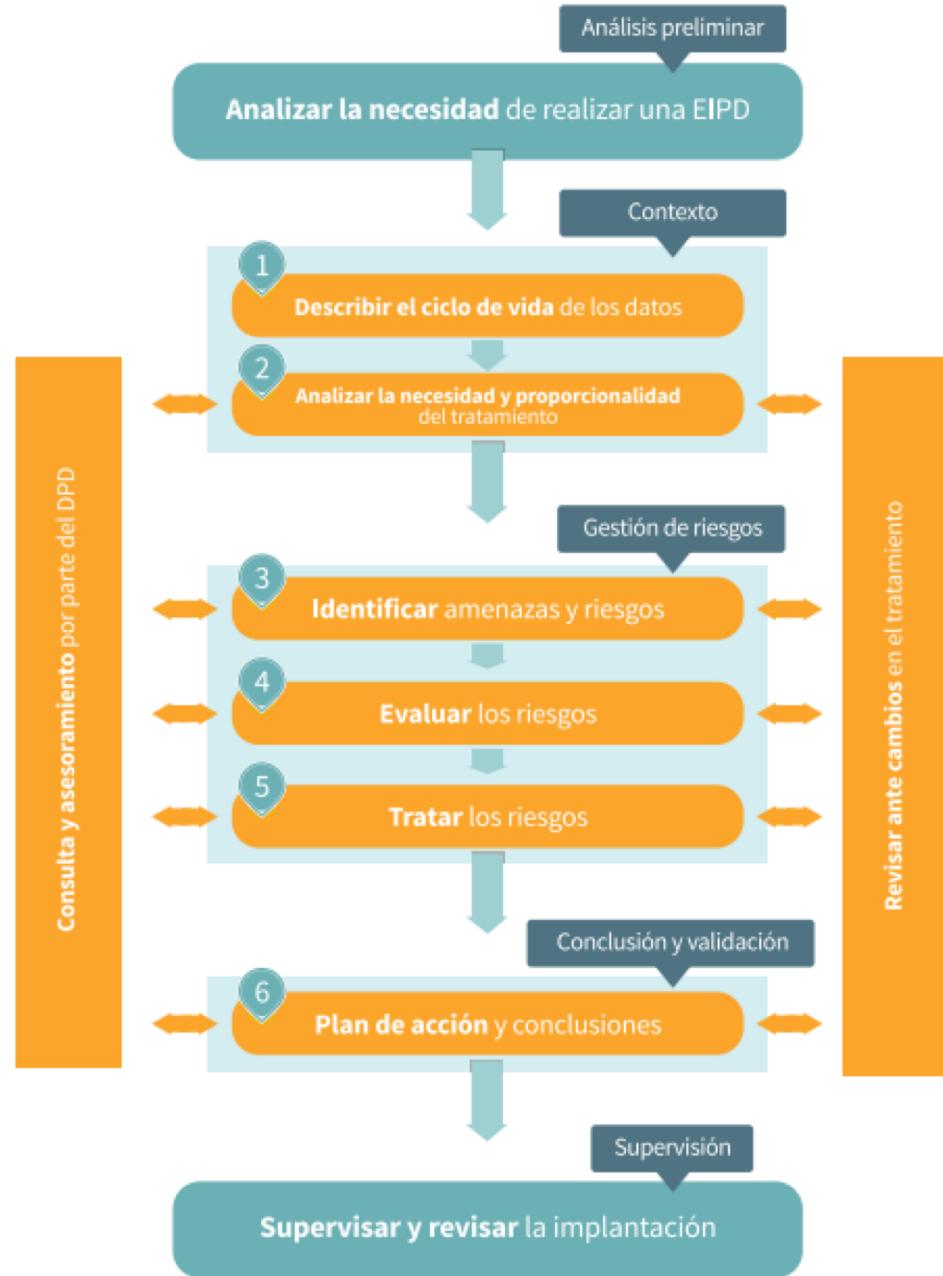
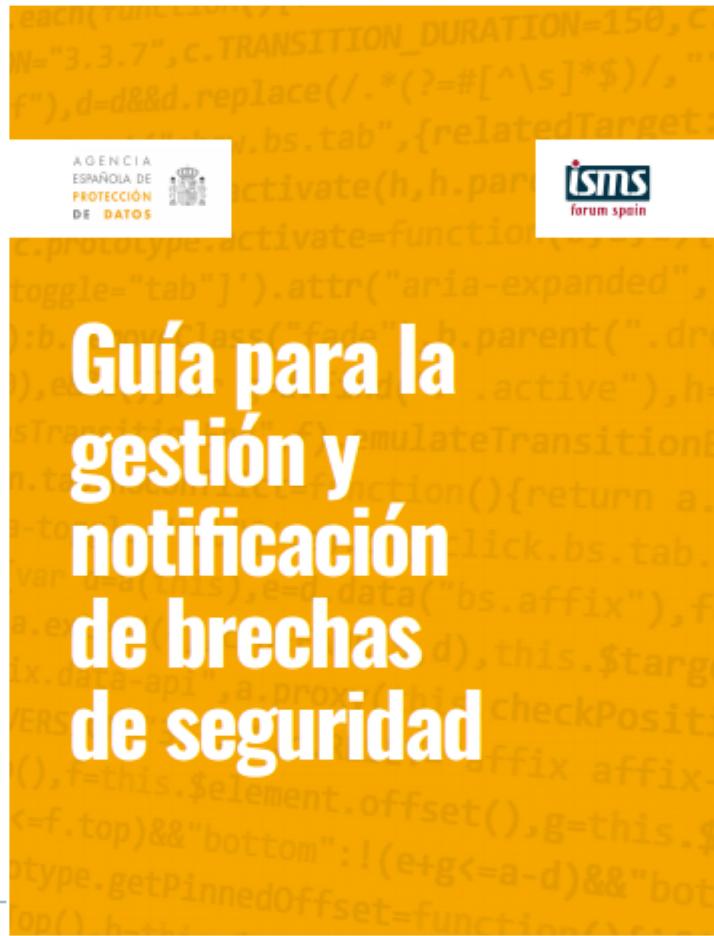
Cargar análisis previos



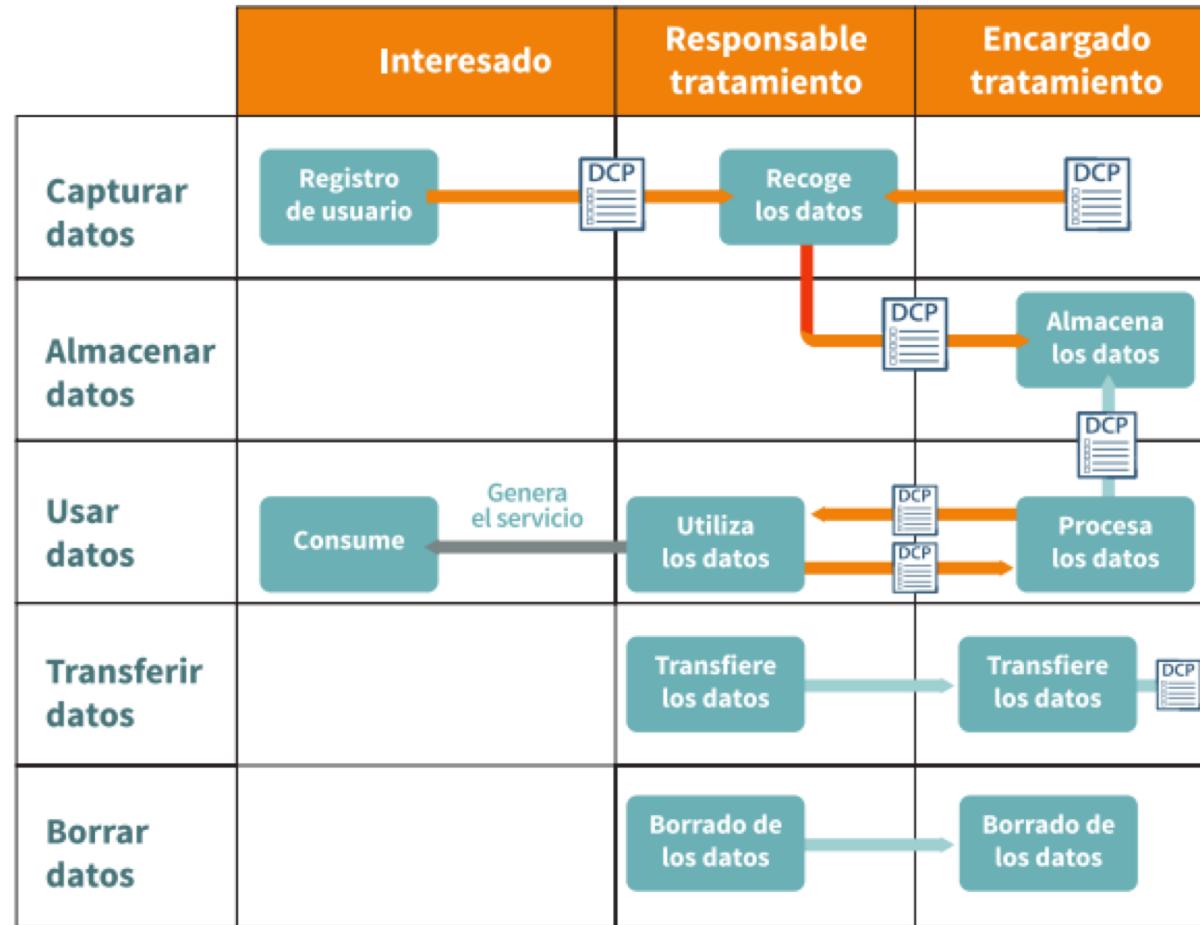
Nombre el análisis



# Etapas EIPD



# Flujo de los datos



Flujo de los datos

Instrucciones

Servicios

# La evaluación de impacto

- ▶ **PIA** (Privacy Impact Assessment).
- ▶ En castellano: **EIPD** Evaluación de Impacto en la Protección de Datos Personales.



**CNIL.**

To protect personal data, support innovation, preserve individual liberties

DATA PROTECTION | TOPICS | THE CNIL |

> The open source PIA software helps to carry out data protection impact assesment



## The open source PIA software helps to carry out data protection impact assesment

12 December 2018

The PIA software aims to help data controllers build and demonstrate compliance to the GDPR. The tools is available in French and in English. It facilitates carrying out a data protection impact assessment, which will become mandatory for some processing operations as of 25 May 2018. This tool also intends to ease the use of the PIA guides published by the CNIL.

**apdcat**  
Autoritat Catalana de Protecció de Dades

## GUÍA PRÁCTICA

(enero de 2018 – versión 2.0)

Evaluación de impacto relativa a la protección de datos

os personales

# Evaluación de impacto



GRUPO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29



17/ES

WP 248 rev.01

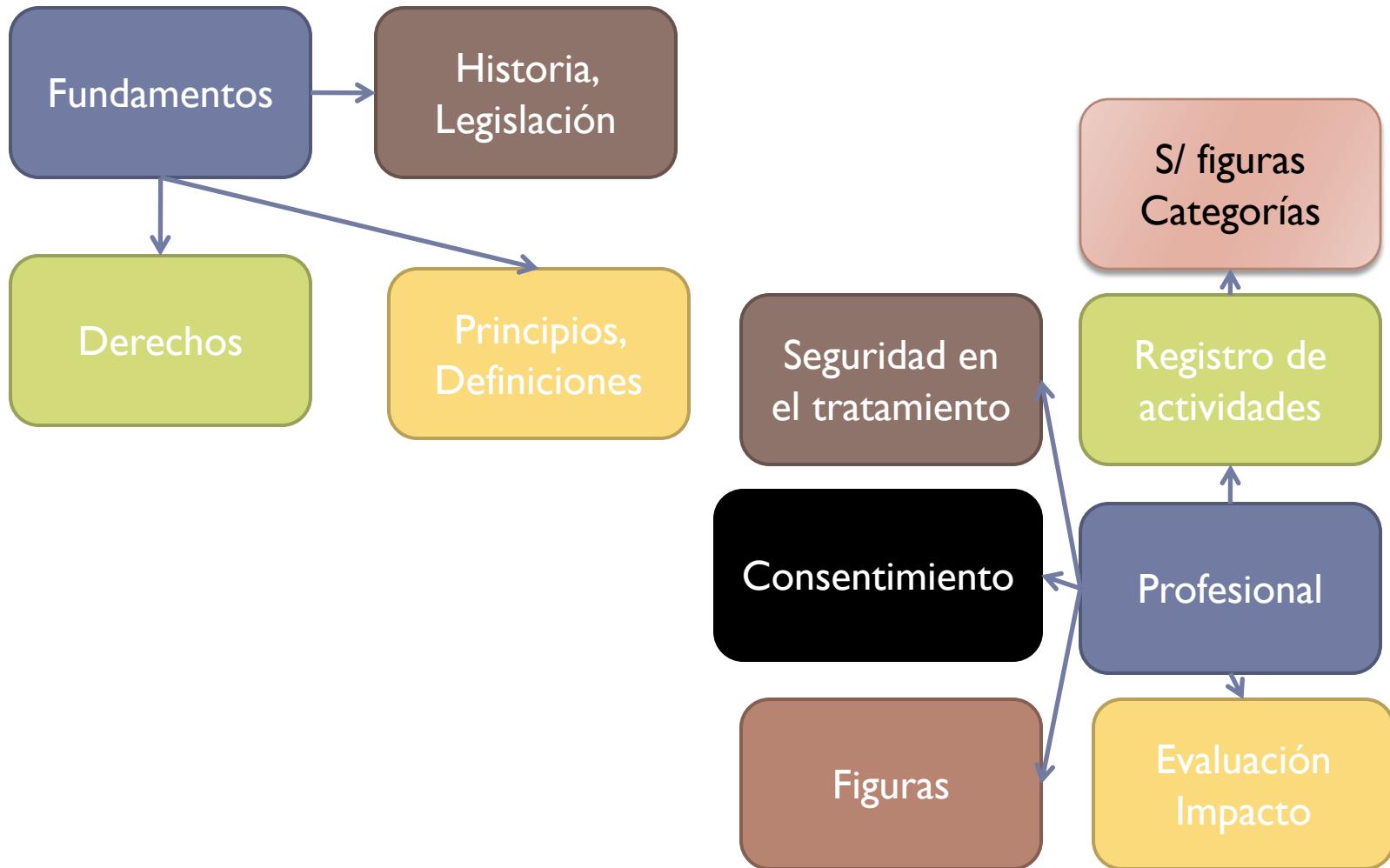
Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679

# Tema 5: Protección de datos personales

---

Juan V. Oltra

La verdad se corrompe tanto con la mentira como con el silencio. *Cicerón*





# Consentimiento

- ▶ Para las personas físicas debe **quedarse totalmente claro que se están recogiendo, utilizando, consultando o tratando** de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.
- ▶ El **principio de transparencia** exige que toda información y comunicación relativa al **tratamiento de dichos datos sea fácilmente accesible y fácil de entender**, y que se utilice un lenguaje sencillo y claro.
  - ▶ **riesgos**, las normas, las salvaguardias y los **derechos** relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento.
  - ▶ **fines** específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida.
- ▶ “**inequívoco**”: se requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado.
- ▶ Tiene que ser verificable.

# ¿Cómo se da el consentimiento?



- ▶ Acto afirmativo claro que refleje una manifestación de voluntad libre:
  - ▶ declaración por escrito,
    - ▶ casilla de un sitio web...
  - ▶ declaración verbal
- ▶ Lo que no:
  - ▶ Silencio o inacción
  - ▶ casillas ya marcadas
  - ▶ Si el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos.

# Condiciones para el consentimiento.



- ▶ El responsable deberá ser capaz de **demostrarlo**.
- ▶ Si se da en una declaración escrita que también se refiera a **otros asuntos**, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.
  - ▶ No será vinculante ninguna parte de la declaración que constituya infracción del Reglamento.
- ▶ El interesado tendrá **derecho a retirar su consentimiento en cualquier momento**. Será tan fácil retirar el consentimiento como darlo.
- ▶ Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la **ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios** para la ejecución de dicho contrato.

# Particularidades. Entorno.

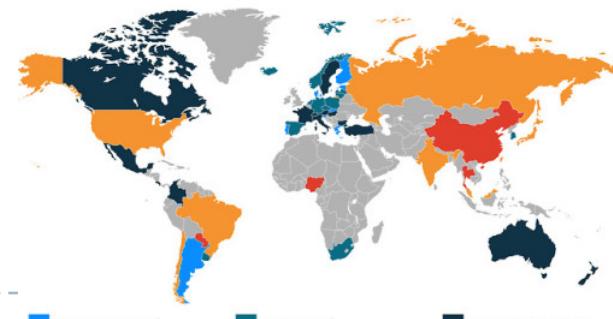
- ▶ Singularidades
  - ▶ Transferencias internacionales
  - ▶ Datos con particularidades
  - ▶ Distribución de las responsabilidades
- ▶ AEPD
- ▶ Ética
- ▶ Derechos digitales



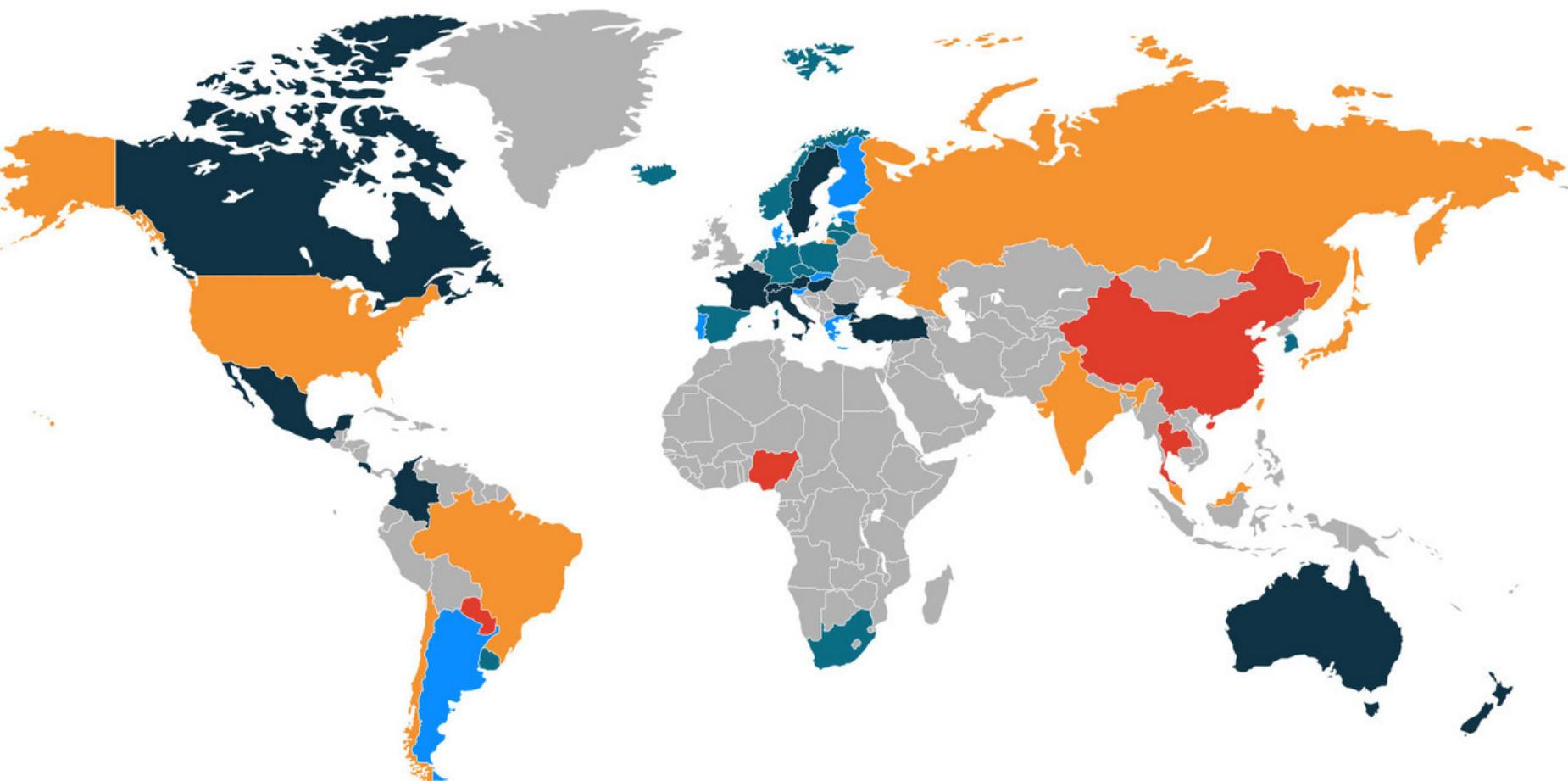
# Transferencias internacionales de datos

- ▶ Solo se podrán realizar transferencias internacionales de datos si el Responsable o Encargado del tratamiento pueden asegurar que el nivel de protección de datos está garantizado mediante
    - ▶ Decisión de adecuación tomada por la Comisión de la UE.
    - ▶ Garantías adecuadas de protección de datos.
  - ▶ Siempre: contrato con el receptor de datos, especificando en el mismo las garantías adecuadas.

If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some interactive voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service provider (currently, Nuance Communications, Inc.) that converts your interactive voice commands to text and to the extent necessary to provide the Voice Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Samsung will collect your interactive



## Privacy and data protection by country



■ Most restricted

■ Restricted

■ Some restrictions

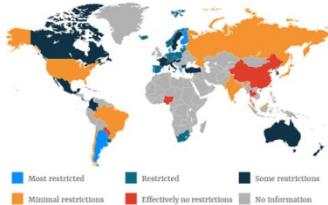
■ Minimal restrictions

■ Effectively no restrictions

■ No information

- ▶ Frente al **interesado**, debe:
    - ▶ Informar la intención de realizar transferencias internacionales.
    - ▶ Verificar la existencia o ausencia de una decisión de adecuación.
    - ▶ Obtener garantías adecuadas y medios para obtener copia de ellas.
  - ▶ De cara al **registro de actividades**:
    - ▶ Identificar las transferencias internacionales.
    - ▶ Documentar la existencia de garantías apropiadas.





# Licitud de las transferencias

Lo dice la comisión de la UE

- Decisión de adecuación de la UE (*Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda*).
- Acuerdos internacionales de privacidad (*Privacy Shield - EEUU*).

AGPD, autonómicas...

- Acuerdos legales entre Organismos públicos.
- Cláusulas tipo o contractuales de protección de datos.
- Mecanismos de certificación.
- Normas corporativas vinculantes.
- Códigos de conducta.

Interesado

- Dio su consentimiento explícito con información de los riesgos.
- Es un contrato con el interesado.
- Se realiza para proteger los intereses vitales de las personas.

Responsable

- Por un interés legítimo e imperioso del Responsable del tratamiento.

# Datos con particularidades

- ▶ Cesión
- ▶ Categorías especiales de datos personales
- ▶ Niños
- ▶ Difuntos



# Cesión



- ▶ Toda revelación de datos realizada **a una persona distinta del interesado**
  - ▶ En la cesión de datos, la organización a quien se le ceden los datos hará en tratamiento por sí misma
  - ▶ En el **tratamiento por terceros**, serán otros los que lo hagan para nosotros.
- ▶ El responsable debe informar sobre la finalidad del fichero, la naturaleza de los datos y el nombre y dirección del cessionario.
- ▶ La realización de tratamientos por cuenta de terceros tiene que estar **regulada en un contrato** que deberá constar preferentemente por escrito, y si no de alguna forma que permita acreditar su acuerdo y contenido. Además debe figurar en el contrato toda aquella medida de seguridad que el encargado del tratamiento está obligado a implementar.
- ▶ Supone un envío de datos de carácter personal a elementos ajenos a la empresa, lleva implícito que todas las partes implicadas en dicha comunicación tengan el **deber de observar secreto**.

# Categorías especiales de datos personales (Artículo 9)



- ▶ Tratamientos **prohibidos**: los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales.
- ▶ Circunstancias **excepcionales**:
  - ▶ Interesado dio su **consentimiento** explícito (si no hay una norma que lo impida);
  - ▶ El tratamiento es necesario en **el ámbito del Derecho laboral** y de la seguridad y protección social,
  - ▶ El tratamiento es necesario para **proteger intereses vitales** del interesado o de otra persona física, si no está capacitado, física o jurídicamente, para dar su consentimiento;
  - ▶ Se realiza por una **fundación, una asociación** o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical;
  - ▶ **Datos personales que el interesado ha hecho manifiestamente públicos**;
  - ▶ Es necesario
    - ▶ Para la formulación, el ejercicio o la defensa de reclamaciones o para los tribunales;
    - ▶ Por razones de un interés público esencial;
    - ▶ Para fines de medicina preventiva o laboral;
    - ▶ Por razones de interés público en el ámbito de la salud pública;
    - ▶ Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

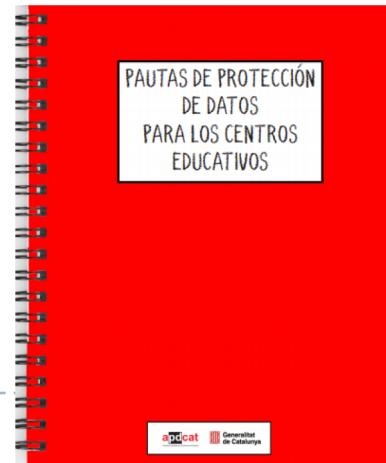


# Niños (Artículo 8)



## ▶ Protección específica

- ▶ De particular importancia cuando se trata del empleo de sus datos con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario.
- ▶ Ofertas directas a niños: es lícito con un **mínimo 16 años**. Si el niño es menor, únicamente si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño.  
**El tope podrá ser rebajado, nunca inferior a 13 años.**



# Fallecidos



- ▶ El Reglamento **no se aplica** a la protección de datos personales de personas fallecidas, aunque los estados miembros pueden establecer normas relativas al respecto.
- ▶ 3/2018:
  - ▶ Se permite que las **personas vinculadas al fallecido por razones familiares o de hecho o sus herederos** puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido.
  - ▶ **No** podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, **cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.**
  - ▶ En caso de fallecimiento de **menores y personas con discapacidad**, estas facultades podrán ejercerse también **por sus representantes legales** o, en el marco de sus competencias, por el Ministerio Fiscal.

# Otros

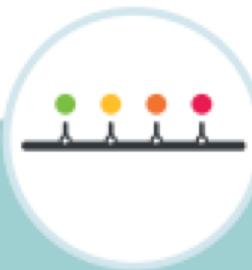
- ▶ Tratamiento con fines de archivo en **interés público**, fines de investigación científica o histórica o fines estadísticos (Artículo 89)
- ▶ Condenas e **infracciones penales**(Artículo 10)
- ▶ Protección de datos en **iglesias** y asociaciones religiosas (Artículo 91)
- ▶ Tratamiento y acceso público de **documentos oficiales** (Artículo 86)



# Hemos sobrevolado las responsabilidades...

- ▶ ¿Cómo se distribuyen entre las distintas figuras?
  - ▶ Responsables, Encargados, DPD's,...
  - ▶ Aparece “RACI”. Figuras de responsabilidad:
- ▶ **Responsible (R):** Responsable de realizar la tarea.
  - ▶ “El que carga con las culpas”
- ▶ **Accountable (A):** Responsable de que la tarea se realice, sin necesidad de ser el que la ejecute y responsable de rendir cuentas sobre su ejecución.
  - ▶ “Al que se le dan y da explicaciones”
- ▶ **Consulted (C):** Figura que debe ser consultada para la realización de la tarea.
  - ▶ “Al que se le consulta”
- ▶ **Informed (I):** Figura que debe ser informada sobre la realización de la tarea.
  - ▶ “Al que se le dice”

# RACI

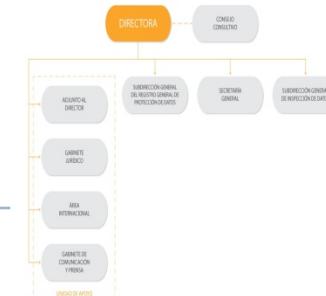


## FASE

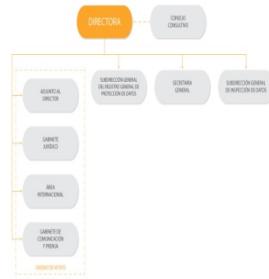
	Responsable del tratamiento	DPD	Encargado del tratamiento	Otras áreas relevantes (pe seguridad, riesgos, Asesoría Jurídica,...)
1 Describir el ciclo de vida de los datos	R/A	C/I	C	C
2 Analizar la necesidad y proporcionalidad del tratamiento	R/A	C/I	C	C
3 Identificar amenazas y riesgos	R/A	C/I	C	-
4 Evaluar los riesgos	R/A	C/I	C	-
5 Tratar los riesgos	R/A	C/I	C	C
6 Plan de acción y conclusiones	R/A	C/I	C	C

# Agencia Española de Protección de Datos (AEPD). Autoridad de control

- ▶ “autoridad pública independiente establecida por un Estado miembro para supervisar la aplicación del Reglamento, para proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión”
- ▶ Es posible que existan **varias autoridades de control** en un Estado miembro; una de ellas será la que represente a dichas autoridades en el Comité (el Comité es un organismo independiente de la Unión con personalidad jurídica, compuesto por el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de Protección de Datos, o por sus respectivos representantes)
- ▶ España: AEPD y autonómicas

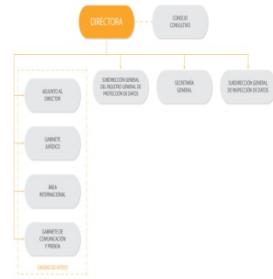


# AEPD y autonómicas

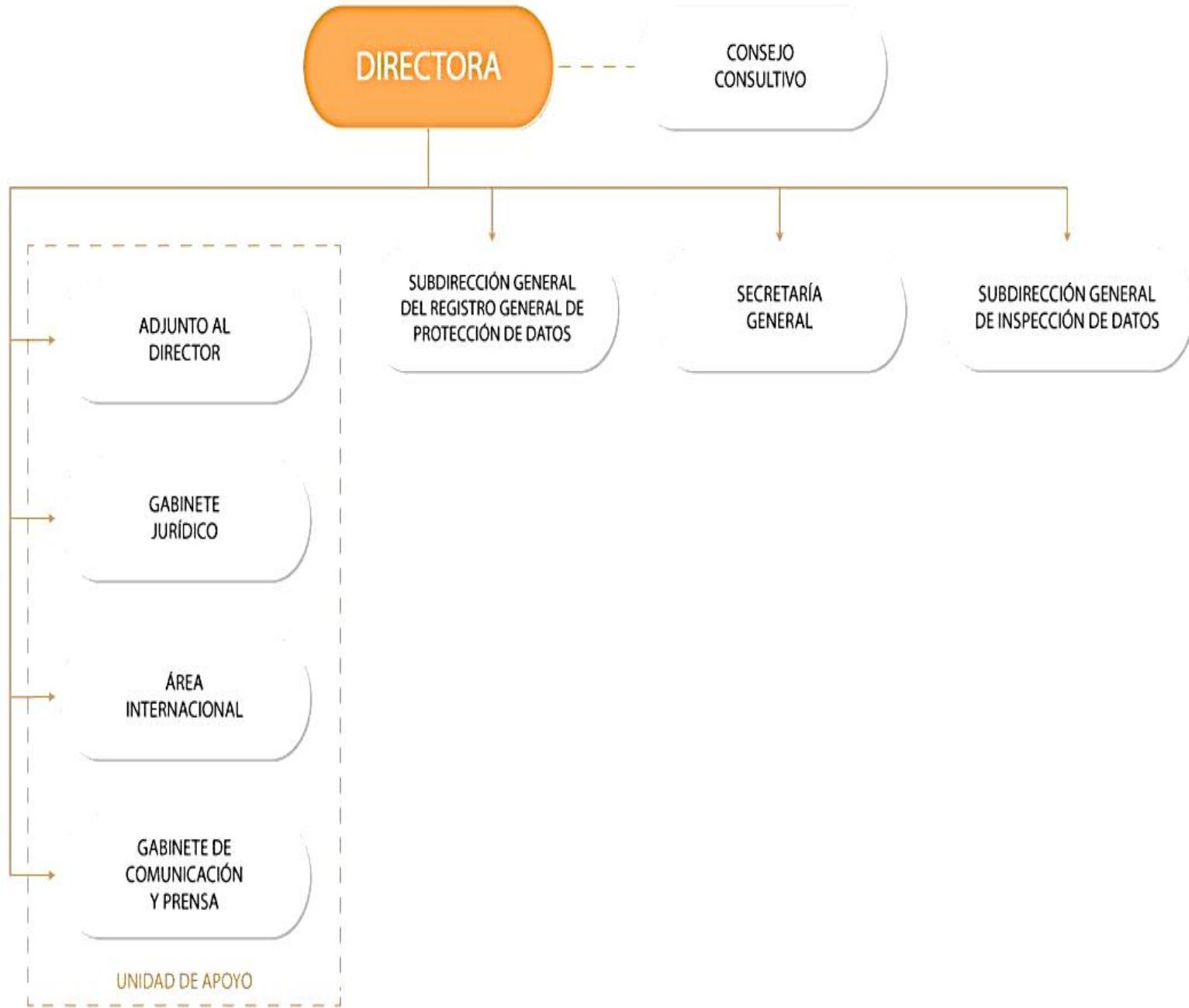


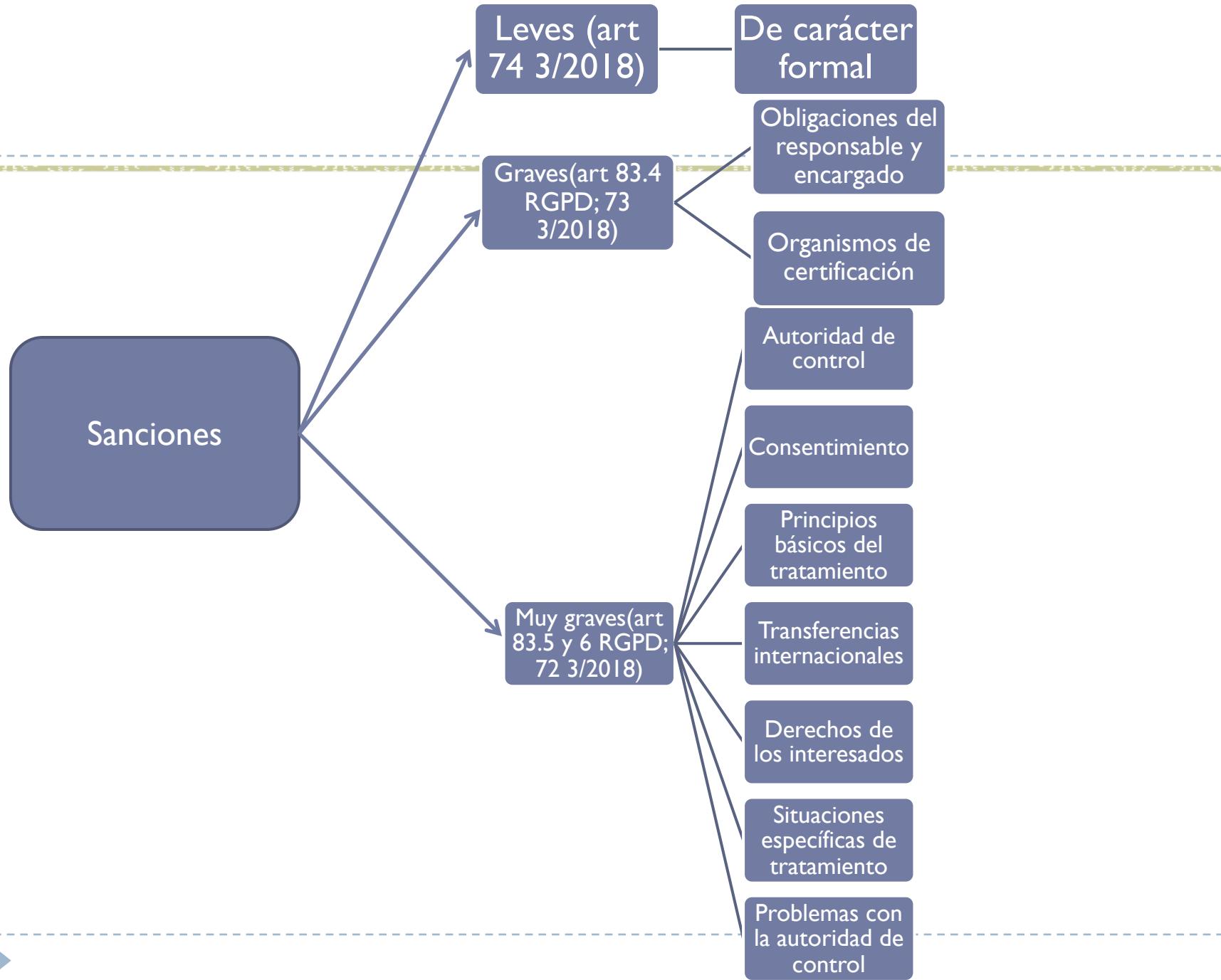
- ▶ Agencia Española de Protección de Datos
  - ▶ Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada. Actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones (lo que no quiere decir que sea totalmente independiente pues quedará sometida al Tribunal de Cuentas).
  - ▶ Finalidad principal: velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación.
- ▶ En España, además, existen agencias de protección de datos de carácter autonómico en Cataluña y en el País Vasco, con un ámbito de actuación limitado a los ficheros de titularidad pública declarados por las Administraciones autonómicas y locales de sus respectivas comunidades autónomas.

# Funciones de la AEPD



- ▶ **Investigación** (en caso de vulneración de la normativa y mediante auditorías preventivas). Administraciones públicas y particulares están obligados a proporcionar informes, antecedentes y justificantes.
- ▶ **Regulación:** Dictando disposiciones que fijen los criterios de actuación: Circulares que son de obligatorio cumplimiento una vez publicadas en el BOE.
- ▶ **Acción exterior:** funciones relacionadas con la acción exterior del Estado en materia de protección de datos. Idem a las comunidades autónomas, a través de las autoridades autonómicas.





# Ética y Protección de datos

- ▶ Algunas razones morales para la protección de los datos personales:
  - ▶ **Prevención de daños** (contraseñas seguras, geolocalización...)
  - ▶ **Evitar la desigualdad informativa.** Las personas suelen estar en posición de desventaja frente a empresas o gobiernos..
  - ▶ **Evitar la injusticia informativa**, que puede conllevar discriminación. La información personal proporcionada en un contexto (médico) puede cambiar su significado en otro contexto (laboral) y desembocar en discriminación.
  - ▶ **No intromisión en la autonomía moral.** La falta de privacidad puede exponer los individuos a fuerzas externas que influyen en sus elecciones.
    - ▶ Fake-news

Living better starts here

Welcome to PatientsLikeMe  
Find answers, support and a path forward with people like you.

[Join the community](#)

600,000+ members	2,800+ conditions	100+ published research studies
------------------	-------------------	---------------------------------

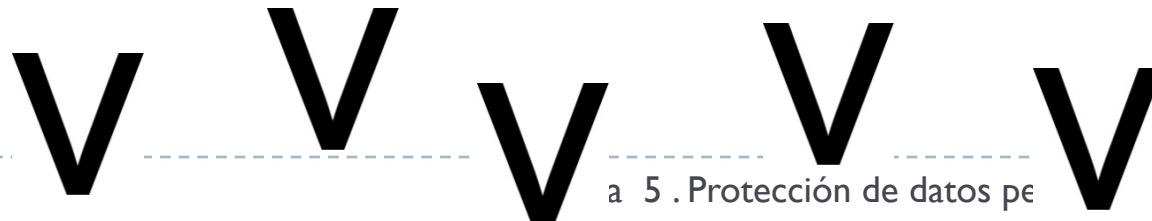


ESTUDIO  
[Fingerprinting o Huella digital del dispositivo](#)



# Taxonomía de la privacidad, por momentos

- ▶ Recolección: vigilancia e interrogación con objeto de captar datos.
- ▶ Proceso: recopilación, identificación, seguridad, uso secundario y exclusión.
- ▶ Difusión: violaciones de confidencialidad, revelación, exposición indebida, facilidad de acceso, chantaje, apropiación y distorsión.
- ▶ Intrusión e interferencia en la toma de decisiones.
  - ▶ ¿Qué caracteriza hoy el uso de las bases de datos? “Las cinco V”: volumen, velocidad, variedad, veracidad y valor.



a 5 . Protección de datos p€

# Códigos de conducta: ética dentro de la ley

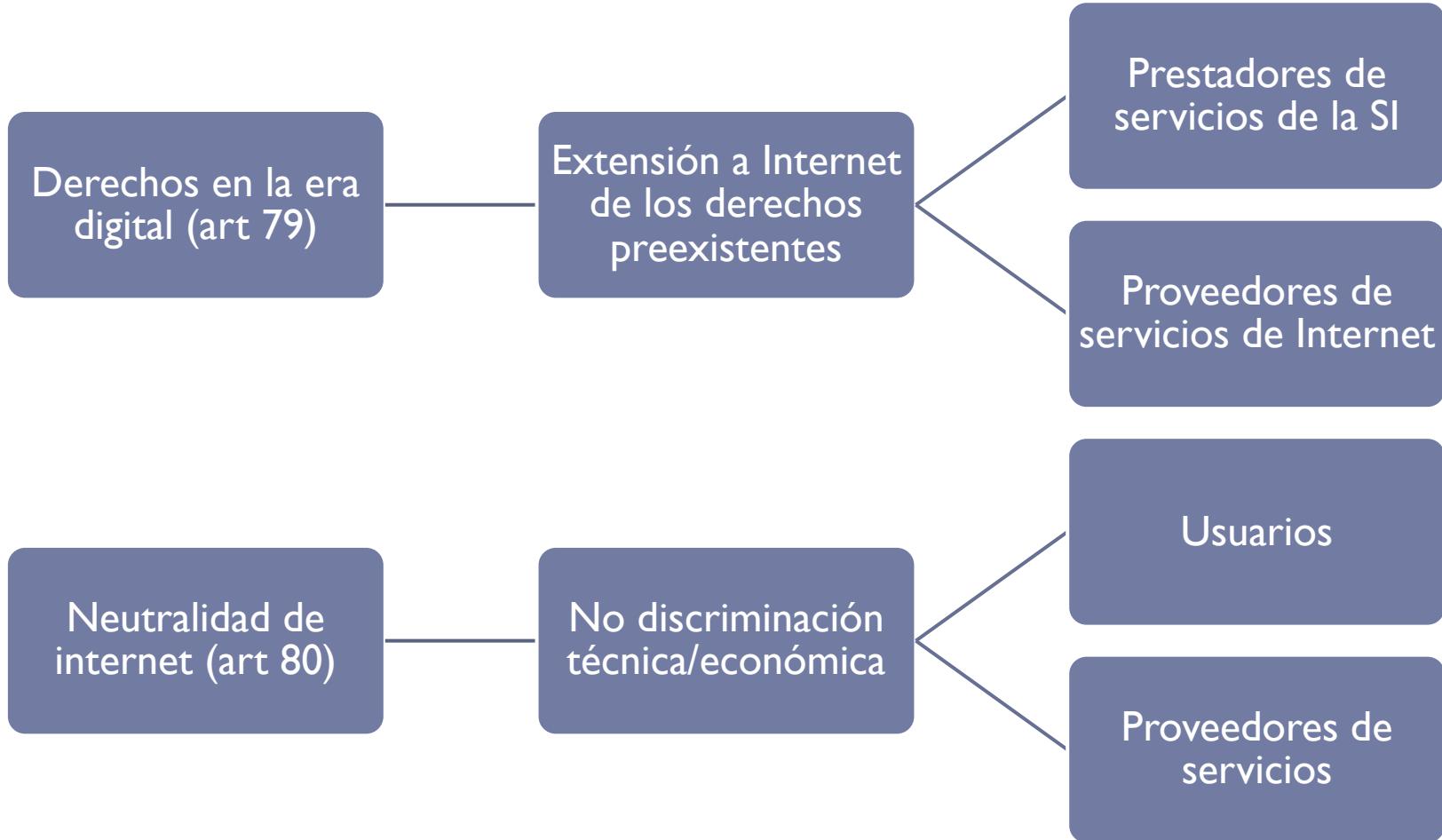


- ▶ Algunos elementos a considerar en estos códigos:
  - ▶ el **tratamiento leal y transparente**;
  - ▶ los **intereses legítimos** perseguidos por los responsables;
  - ▶ la **recogida** de datos personales;
  - ▶ la **seudonimización** de datos personales;
  - ▶ la **información proporcionada** al público y a los interesados;
  - ▶ el ejercicio de los **derechos** de los interesados;
  - ▶ la información proporcionada a los **niños** y la protección de estos;
  - ▶ la **notificación de violaciones** de la seguridad de los datos personales
  - ▶ la transferencia de datos personales a **terceros países**

# Derechos digitales. Título X

- ▶ Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, **elevar a rango constitucional una nueva generación de derechos digitales**. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.
- ▶ La estructura del título y los nuevos derechos podemos verlos en los siguientes esquemas:

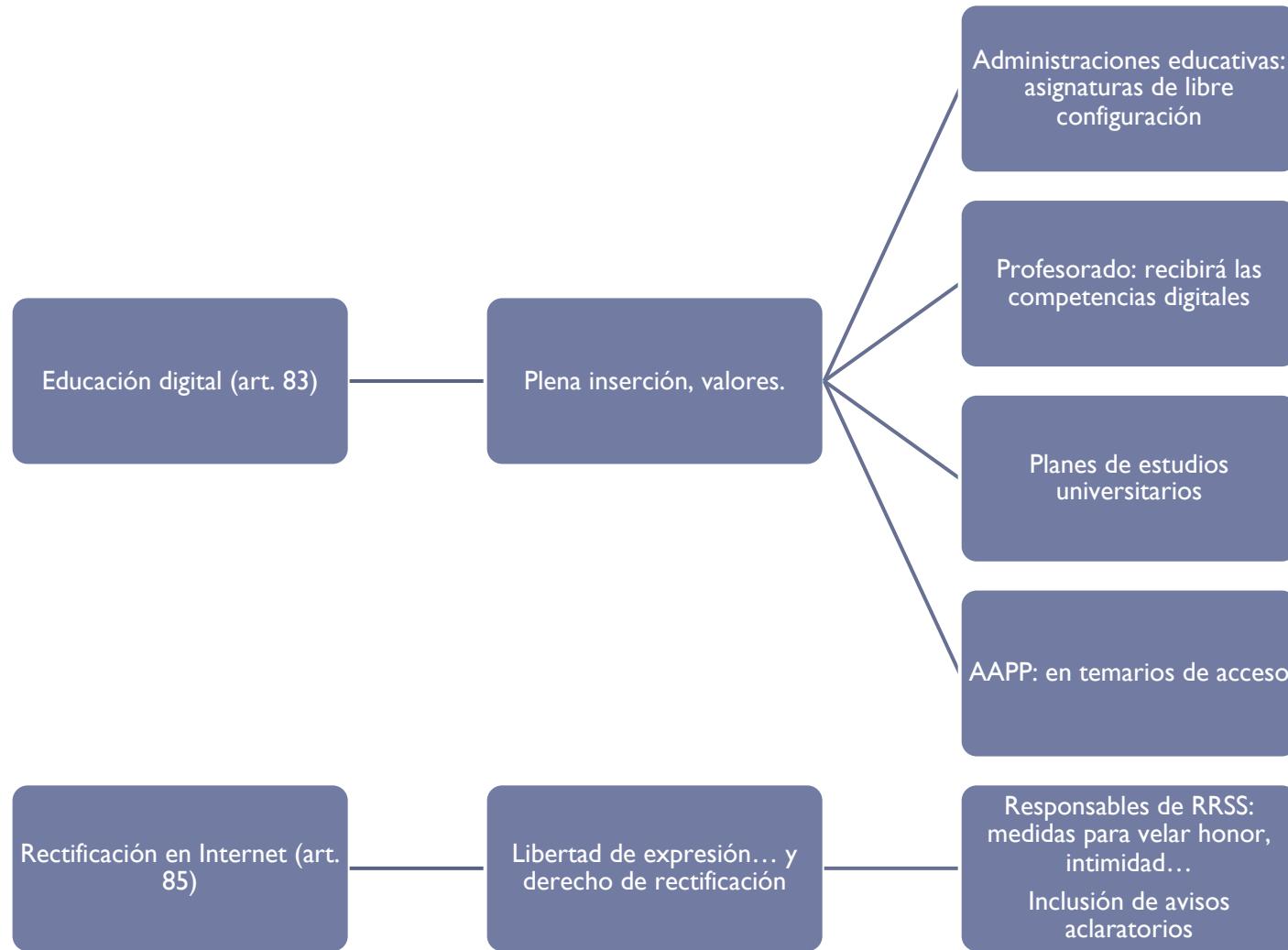
# Derechos en la era digital / Neutralidad



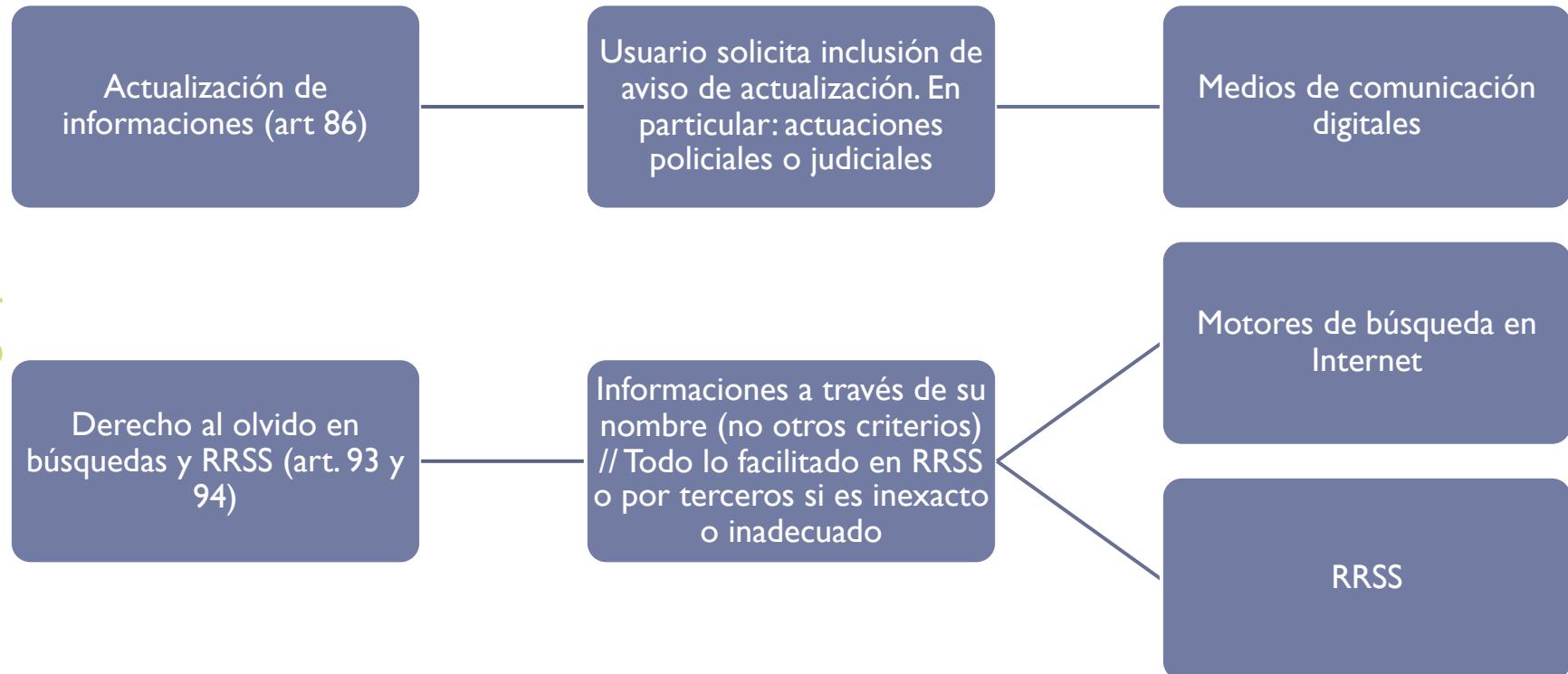
# Acceso universal / Seguridad digital



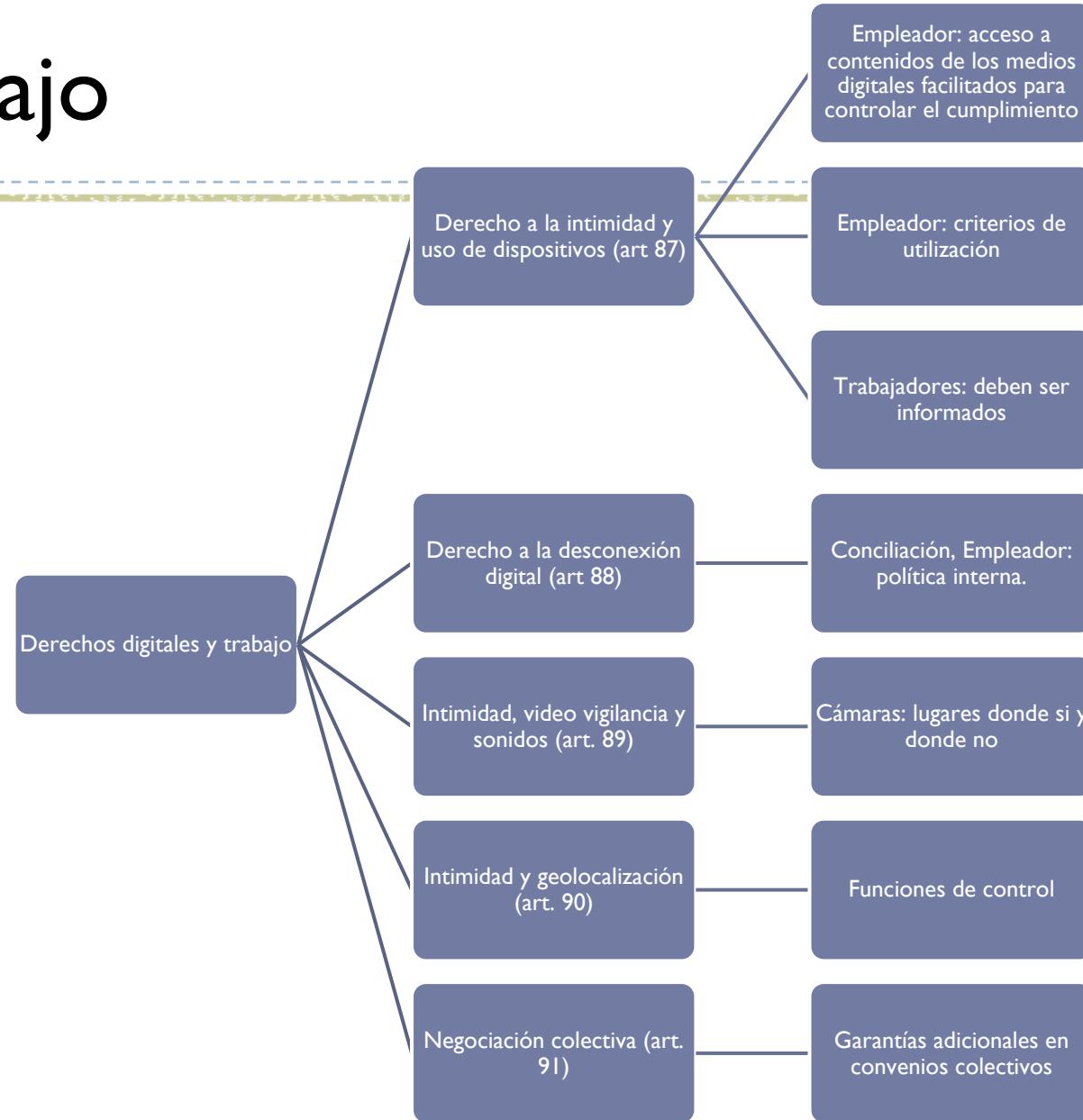
# Educación digital / Rectificación



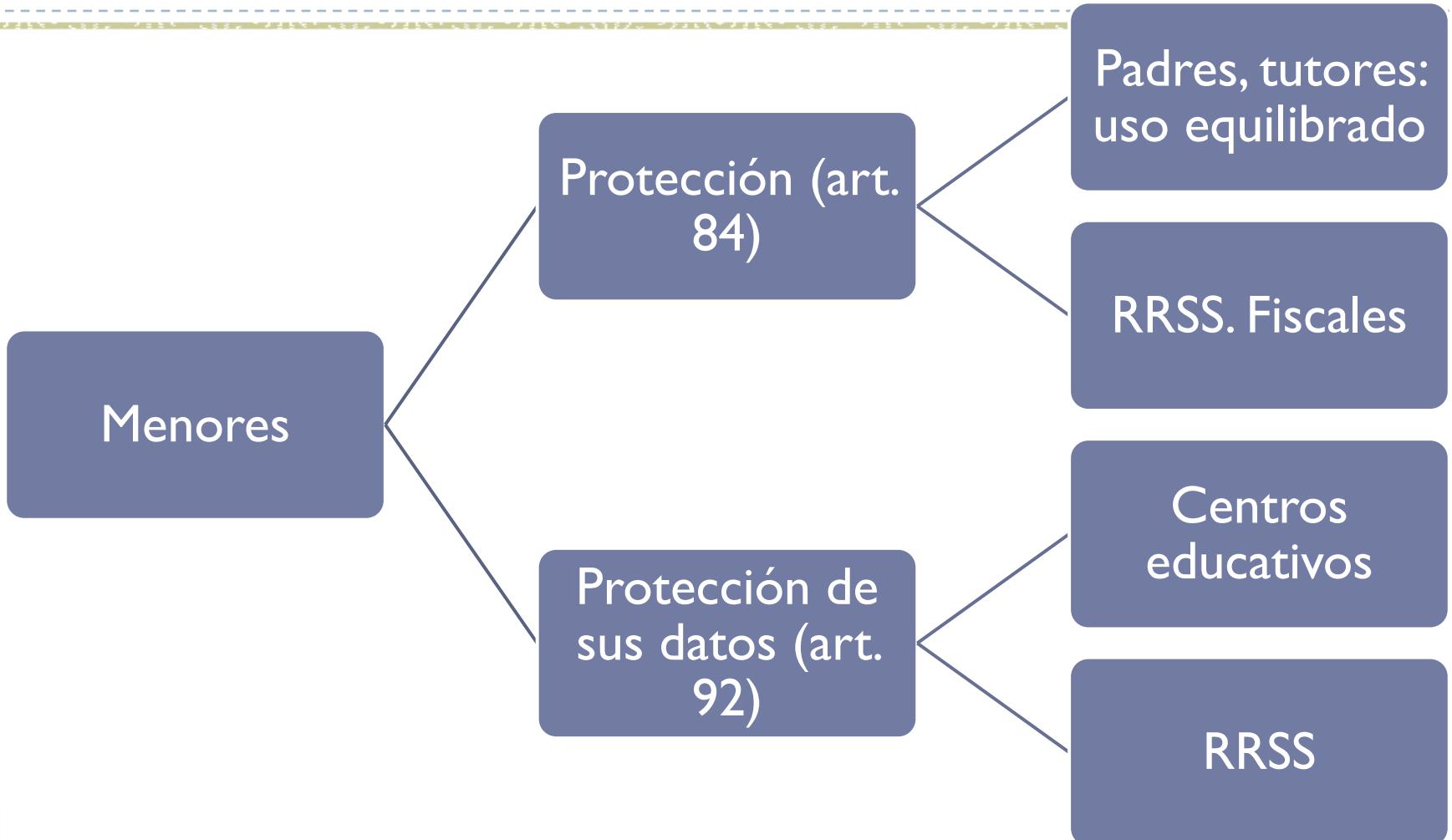
# Actualización de informaciones / Derecho al olvido (la vimos)



# Trabajo



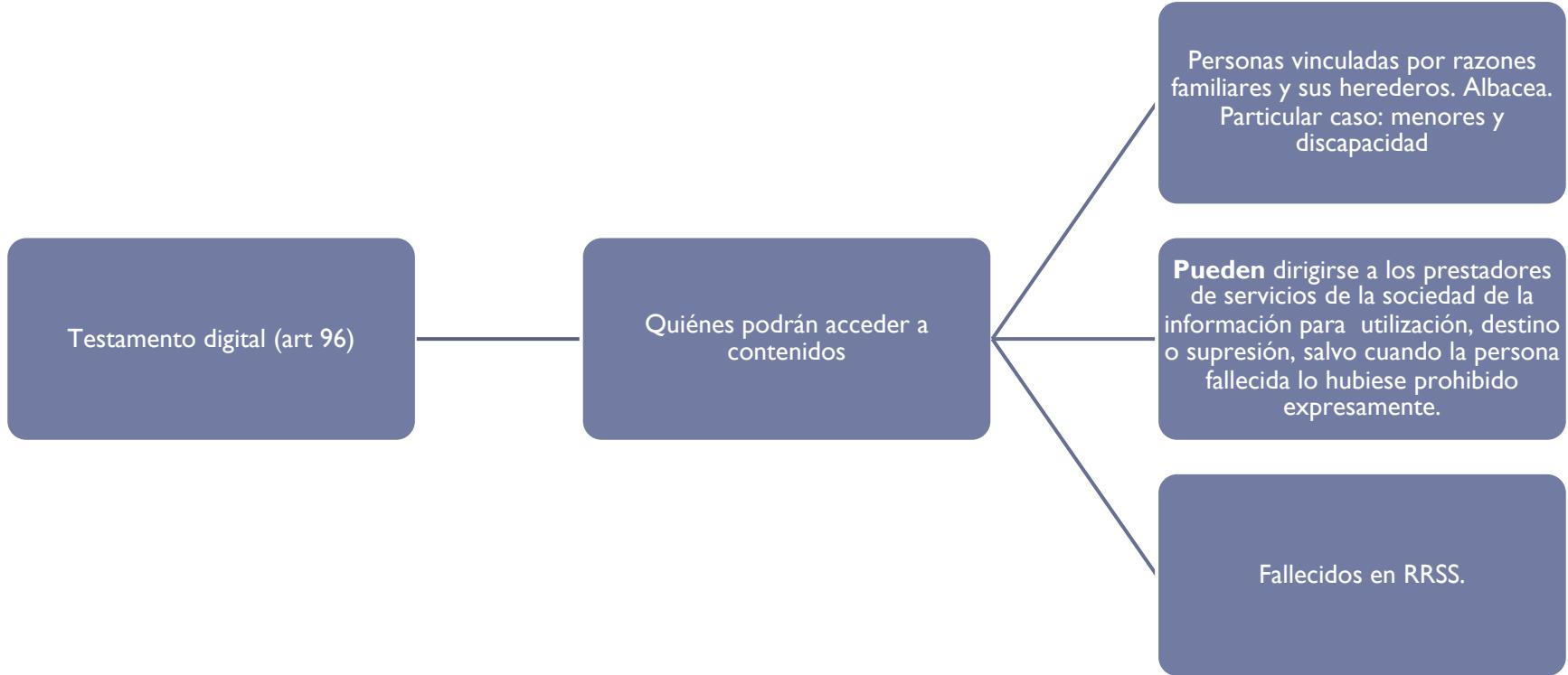
# Menores



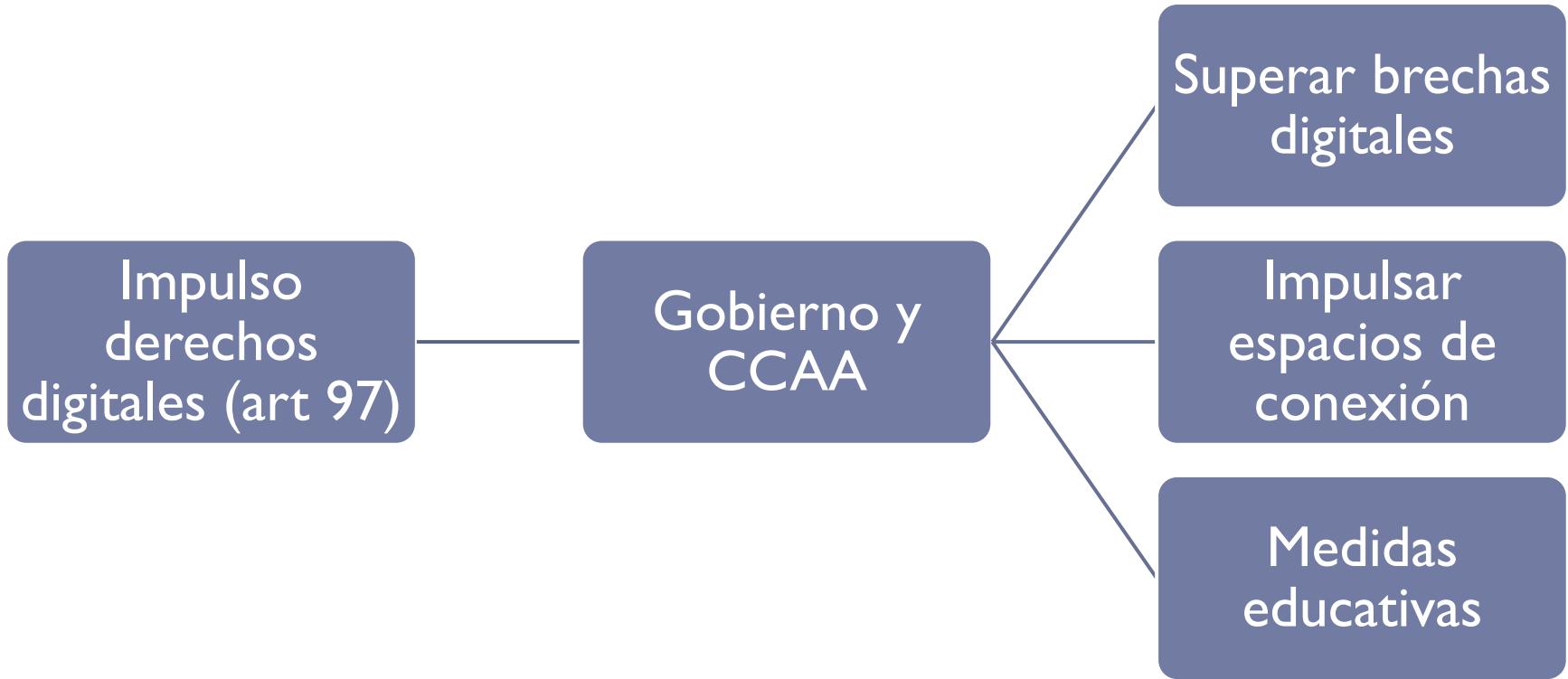
# Portabilidad en RRSS



# Testamento digital



# Impulso

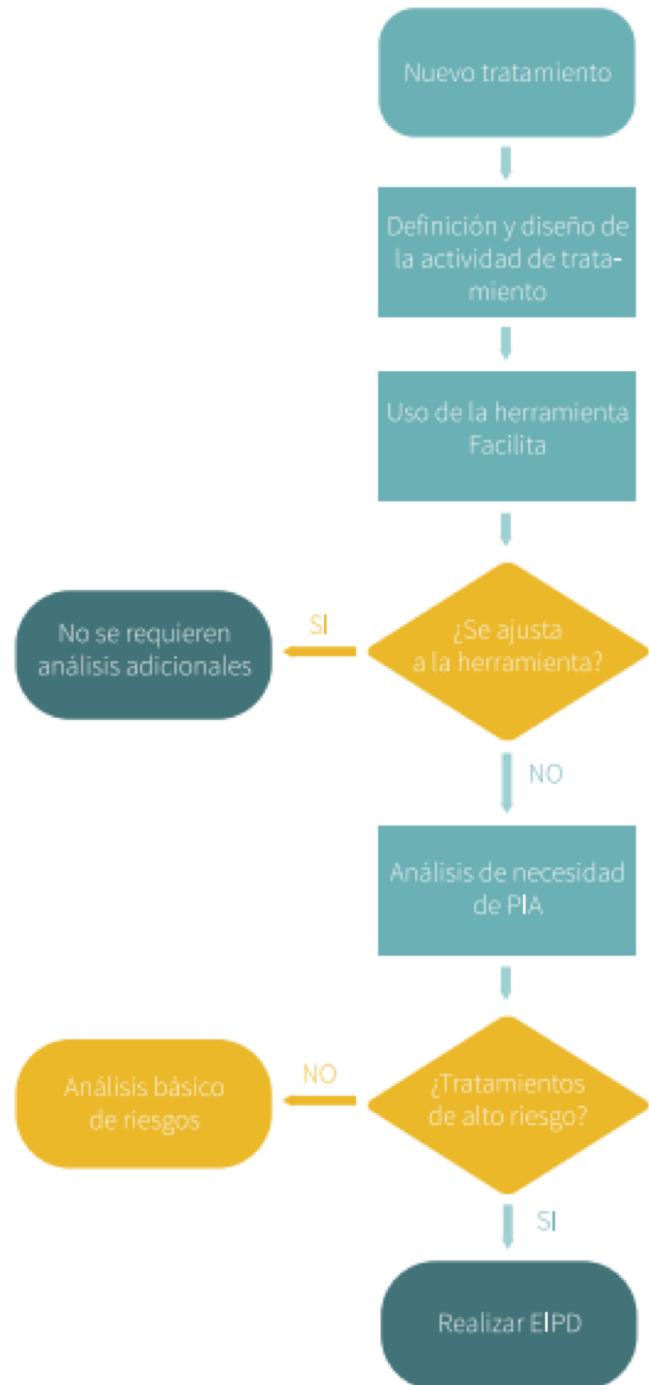


# Anexo – Para profundizar

- ▶ Pasos.
  - ▶ 1. Principios relativos al tratamiento
  - ▶ 2. Licitud del tratamiento
  - ▶ 3. Tratamiento de categorías especiales
  - ▶ 4. Derechos del interesado. Transparencia
  - ▶ 5. Responsabilidad del responsable
  - ▶ 6. Protección de datos desde el diseño y por defecto
  - ▶ 7. Tratamiento
    - ▶ 7.1. Brechas de seguridad
    - ▶ 7.2. Riesgos
  - ▶ 8. DPD
  - ▶ 9. Transferencias internacionales

# 1. Principios relativos tratamiento

- ▶ Implantación de medidas de seguridad
- ▶ Trazabilidad de los fines
- ▶ Calidad de los datos
  - ▶ ¿medidas de seguridad previas?
  - ▶ Aparece la evaluación de impacto...



## 2. Licitud del tratamiento

- ▶ Necesidad del mismo
- ▶ Consentimiento
  - ▶ Tenemos claros los principios relativos al tratamiento
    - ▶ Finalidad
    - ▶ Legitimidad
    - ▶ Exactitud
    - ▶ Integridad
    - ▶ Confidencialidad
    - ▶ Licitud del tratamiento

GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS



17/ES  
WP259 y rev.01

Grupo de trabajo del artículo 29

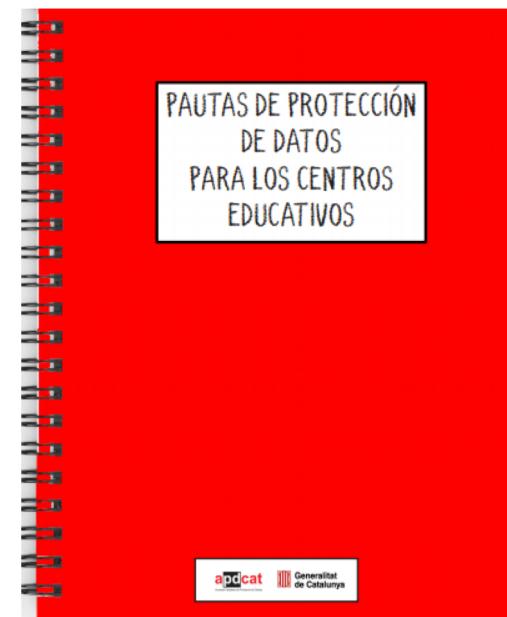
Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679

adoptadas el 28 de noviembre de 2017

revisadas por última vez y adoptadas el 10 de abril de 2018

### 3. Tratamiento de categorías especiales

- ▶ Medicina preventiva o laboral
  - ▶ Salud, política, religión...
- ▶ Interés público
- ▶ Condenas e infracciones penales



INTERNATIONAL  
STANDARD      ISO/IEC  
29187-1

First edition  
2013-02-15

---

**Information technology — Identification of privacy protection requirements pertaining to learning, education and training (LET) —**

**Part 1:  
Framework and reference model**

*Technologies de l'information — Identification des exigences de protection privée concernant l'apprentissage, l'éducation et la formation (AEF) —*

*Partie 1: Cadre général et modèle de référence*

protección de datos personales

## 4. Derechos del interesado. Transparencia

- ▶ Informar
- ▶ Como, cuando
- ▶ A quien
- ▶ Gestión de los derechos: que, como, donde, cuando...
  - ▶ Portabilidad: formato estructurado, uso común, lectura mecánica...
  - ▶ Perfiles, decisiones individuales automatizadas...



# 5. Responsabilidad del responsable

- ▶ Contratos con encargado
- ▶ Riesgos y su probabilidad
- ▶ Medidas revisadas
- ▶ Políticas de protección de datos
- ▶ Los corresponsables
- ▶ Autorizaciones previas



# 6. Protección de datos desde el diseño y por defecto

- ▶ Antes de determinar el tratamiento
- ▶ Medidas técnicas y organizativas
- ▶ Solo los datos necesarios
- ▶ **Ejemplos:**

- ▶ **Protección de datos desde el diseño**

El uso de seudonimización (sustitución del material de identificación personal) y de cifrado (codificación de mensajes de forma que solo las personas autorizadas puedan leerlos).

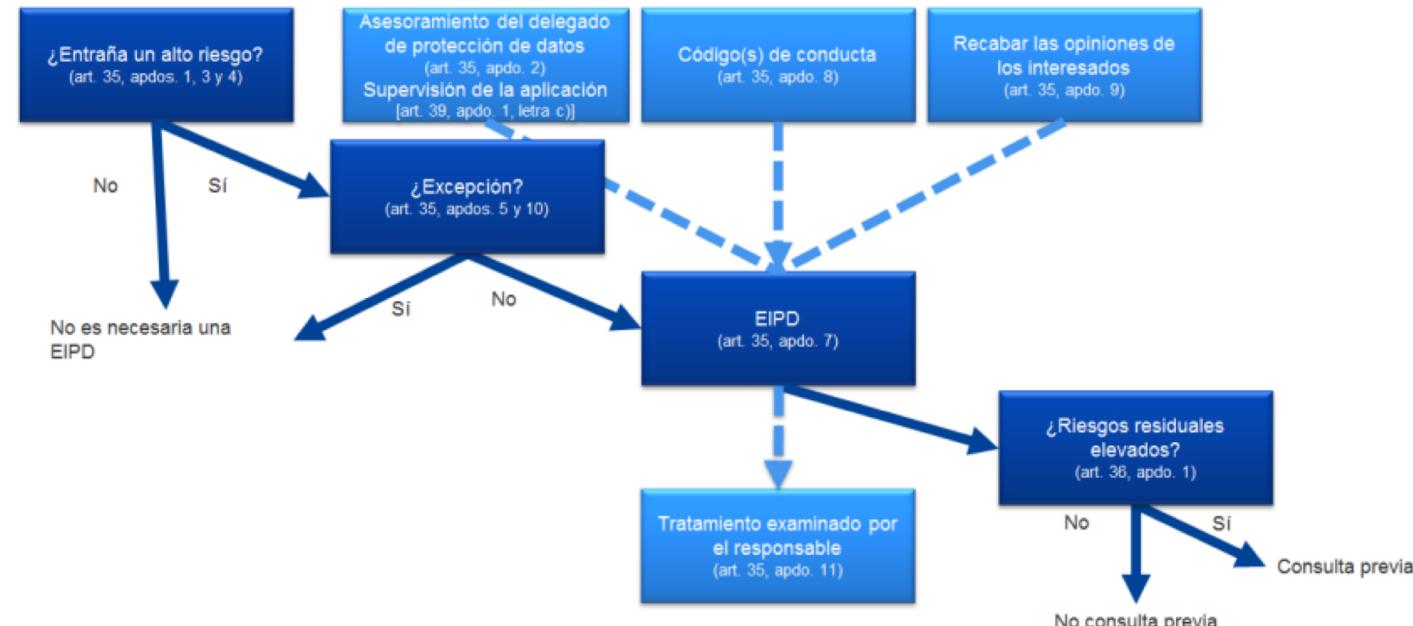
- ▶ **Protección de datos por defecto**

Debería animarse a una plataforma de redes sociales a configurar los parámetros del perfil de los usuarios en el entorno que más proteja la intimidad, por ejemplo limitando desde el primer momento la accesibilidad del perfil de los usuarios para que por defecto no sea accesible a un número indefinido de personas.

LISTADO DE ADMITIDOS		
DNI	NOTA MEDIA	Número
16618796P	5,747	150
16625573T	7,935	28
16627818Z	7,904	51
44619336A	6,000	178
44632213T	7,700	19
44635337L	6,754	164
44642345N	7	160
44642602Q	6,173	175
44642943N	6,02	131
44643519J	6,625	167

# 7. Tratamiento

- ▶ Registro de las actividades
- ▶ Seguridad del tratamiento.
  - ▶ Evaluación de Impacto
  - ▶ Medidas técnicas y organizativas
- ▶ Notificación de las brechas de seguridad



# 7.1. Brechas de seguridad

## ▶ Gestión de las brechas de seguridad

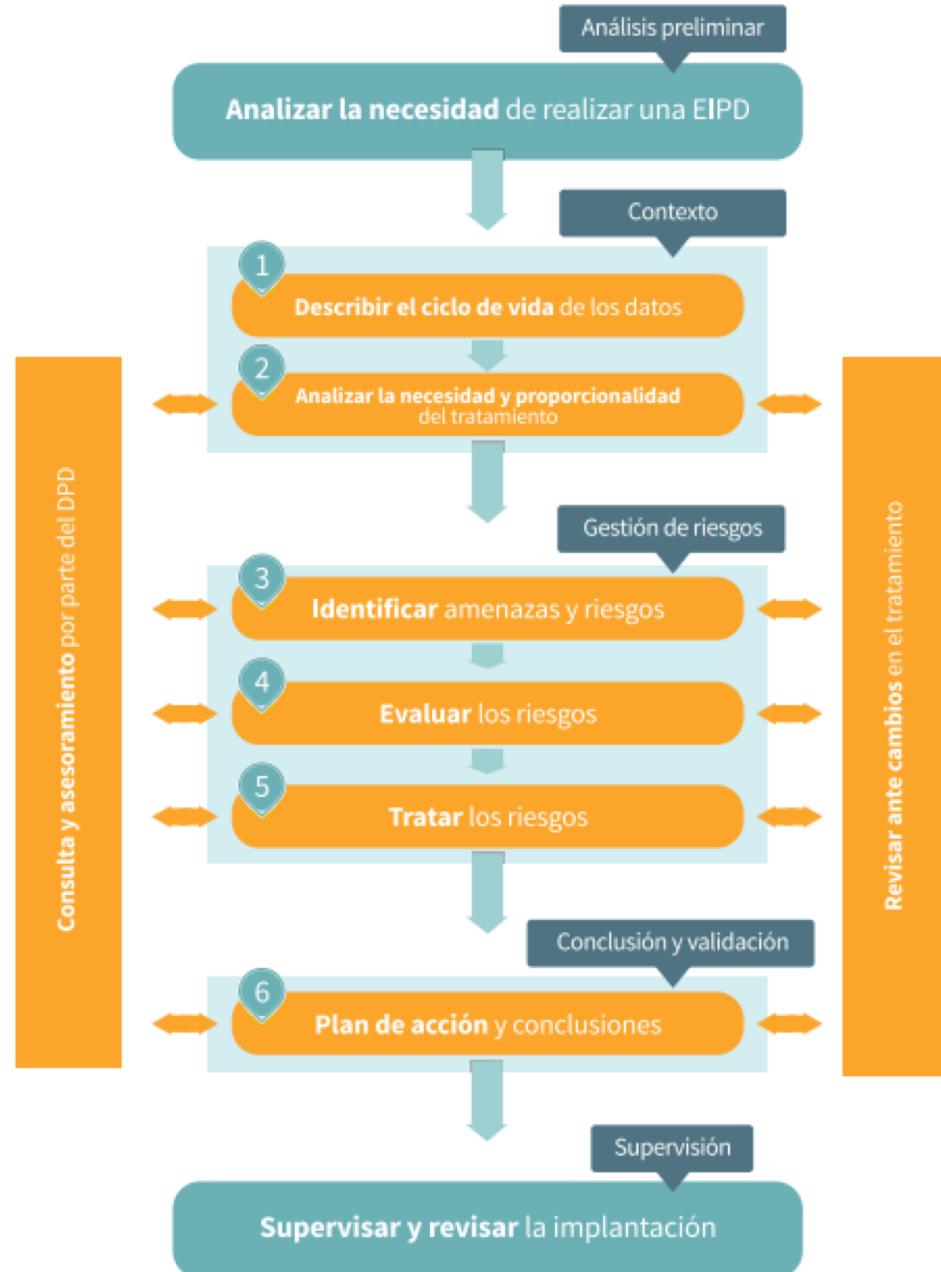
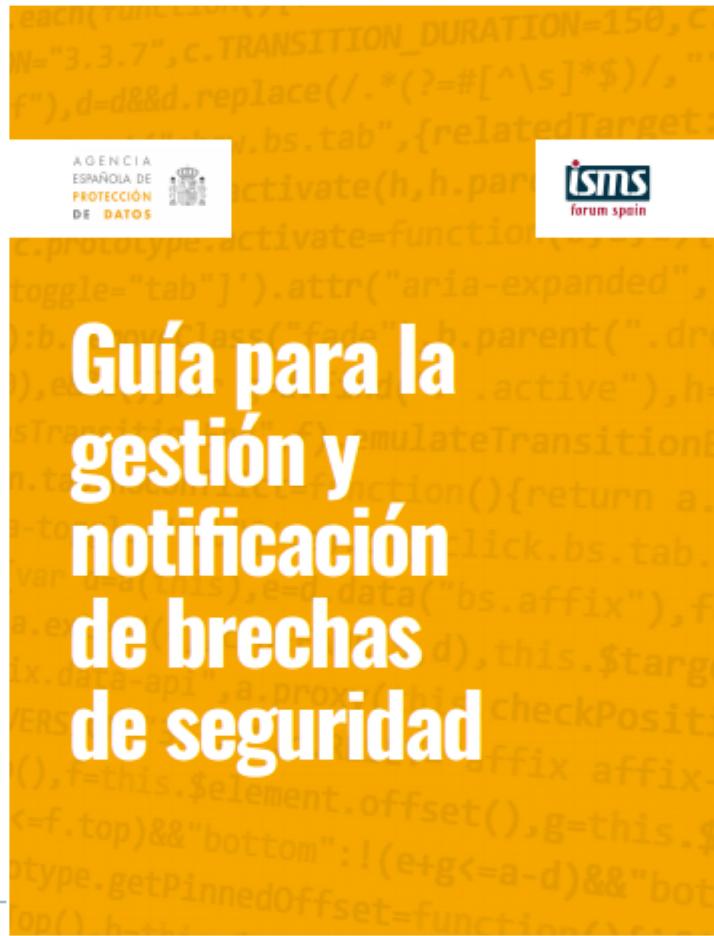


Procedimiento de Gestión de Incidentes de Seguridad (GDPR)



PROC-CORP-05

# Etapas EIPD



# 7.1. Brechas de seguridad

## Notificación de la brecha

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29



18/ES

WP250rev.01

**Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679**

AGENCIA  
ESPAÑOLA DE  
PROTECCIÓN  
DE DATOS



FORMULARIO NOTIFICACIÓN  
BRECHAS DE SEGURIDAD

### 1. Datos de la notificación

Tipo de notificación:  Inicial,  Adicional,  Completa  
Referencia notificación inicial: \_\_\_\_\_ Fecha notificación inicial: \_\_\_\_\_

### 2. Identificación del Delegado de Protección de Datos o persona de contacto

NIF/NIE: \_\_\_\_\_ Nombre: \_\_\_\_\_  
Apellidos: \_\_\_\_\_ Cargo: \_\_\_\_\_  
Dirección: \_\_\_\_\_ C.P.: \_\_\_\_\_  
Provincia: \_\_\_\_\_ Localidad: \_\_\_\_\_  
Teléfono(s): \_\_\_\_\_ / \_\_\_\_\_ e-mail: \_\_\_\_\_

### 3. Identificación del responsable del tratamiento

Nombre de la Organización: \_\_\_\_\_  
Tipo de Organización:  Privada,  Pública  
CIF: \_\_\_\_\_ Dirección distinta del DPD o persona de contacto:   
Dirección: \_\_\_\_\_ C.P.: \_\_\_\_\_  
Provincia: \_\_\_\_\_ Localidad: \_\_\_\_\_  
Teléfono(s): \_\_\_\_\_ / \_\_\_\_\_ e-mail: \_\_\_\_\_

### 4. Identificación del encargado del tratamiento

¿Hay otra organización implicada en la brecha de seguridad?   
Nombre de la Organización: \_\_\_\_\_  
Tipo de Organización:  Privada,  Pública  
CIF: \_\_\_\_\_  
Dirección: \_\_\_\_\_ C.P.: \_\_\_\_\_  
Provincia: \_\_\_\_\_ Localidad: \_\_\_\_\_  
Teléfono(s): \_\_\_\_\_ / \_\_\_\_\_ e-mail: \_\_\_\_\_

### 5. Información temporal de la brecha

Fecha detección de la brecha: \_\_\_\_\_  Exacta,  Estimada.  
Medios de detección de la brecha:

# 7.1. Brechas de seguridad

- ▶ ¿Qué normas debemos tener en cuenta si descubrimos una brecha de seguridad?

**norma  
española**

UNE 71505-1

Julio 2013

TÍTULO	Tecnologías de la Información (TI)  Sistema de Gestión de Evidencias Electrónicas (SGEE)  Parte 1: Vocabulario y principios generales
--------	---

**norma  
española**

UNE 71505-2

Julio 2013

TÍTULO	Tecnologías de la Información (TI)  Sistema de Gestión de Evidencias Electrónicas (SGEE)  Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas
--------	--

**norma  
española**

UNE 71505-3

Julio 2013

TÍTULO	Tecnologías de la Información (TI)  Sistema de Gestión de Evidencias Electrónicas (SGEE)  Parte 3: Formatos y mecanismos técnicos
--------	---

## 7.1. Brechas de seguridad

- ▶ ¿Qué normas debemos tener en cuenta si descubrimos una brecha de seguridad?

L 173/2

ES

Diario Oficial de la Unión Europea

26.6.2013

### REGLAMENTOS

#### REGLAMENTO (UE) N° 611/2013 DE LA COMISIÓN de 24 de junio de 2013

relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas

# 7.1. Brechas de seguridad

- ▶ ¿Qué normas debemos tener en cuenta si descubrimos una brecha de seguridad?

INTERNATIONAL  
STANDARD

ISO/IEC  
**29100**

First edition  
2011-12-15

INTERNATIONAL  
STANDARD

ISO/IEC  
**29147**

First edition  
2014-02-15

---

**Information technology — Security  
techniques — Privacy framework**

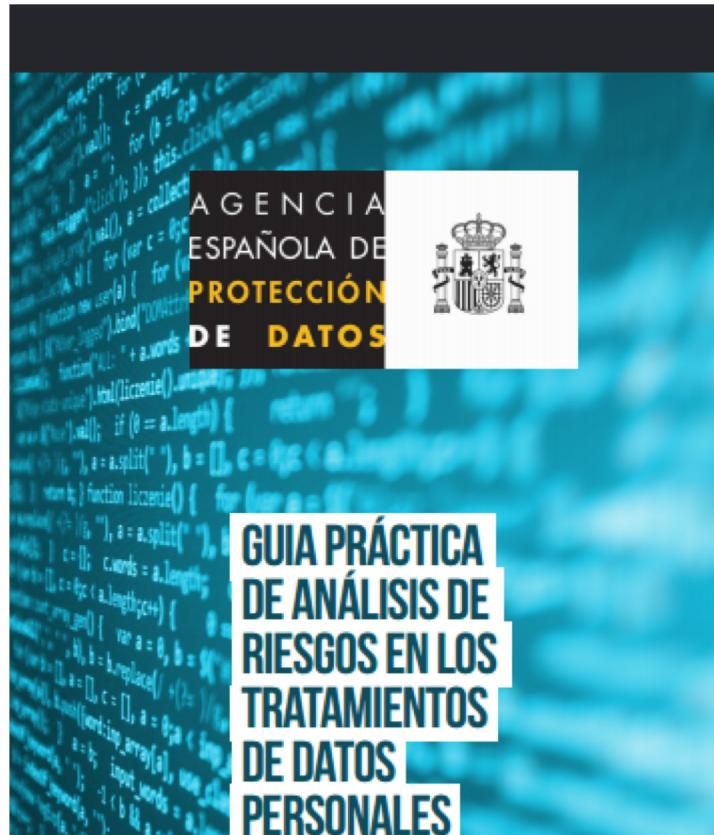
*Technologies de l'information — Techniques de sécurité — Cadre privé*

---

**Information technology — Security  
techniques — Vulnerability disclosure**

*Technologies de l'information — Techniques de sécurité —  
Divulgation de vulnérabilité*

## 7.2. Riesgos



Riesgo = Probabilidad X Impacto

## 7.2. Riesgos



# 7.2. Riesgos

## Ejemplos de amenazas

Tipo de amenaza	Amenaza	¿Qué preguntas se pueden formular para identificar la amenaza?
 Acceso ilegítimo a los datos	<ul style="list-style-type: none"> <li>■ Perdidas de dispositivos móviles</li> <li>■ Fuga de información</li> <li>■ Acceso intencionado por parte de personal no autorizado</li> <li>■ Ataques intencionados (hacking, suplantación de identidad, etc.)</li> <li>■ Uso ilegítimo de datos personales</li> </ul>	<ul style="list-style-type: none"> <li>• ¿Los dispositivos móviles y de almacenamiento están cifrados?</li> <li>• ¿Existen métodos para extraer la información durante la operación de tratamiento?</li> <li>• ¿Está expuesta la información al acceso por parte de terceros no autorizados? ¿Existe un mecanismo para dar acceso a los datos únicamente al personal autorizado?</li> <li>• La operación de tratamiento es susceptible de ataques de hacking? ¿Es susceptible de ataques de phishing o de otros métodos de suplantación de identidad?</li> <li>• ¿Existe una adecuada gestión de la configuración de los parámetros de seguridad de los elementos (elementos de red, SO y BBDD)</li> <li>• ¿Existe una base legitimadora para la actividad de tratamiento? ¿Las finalidades de las actividades de tratamiento son necesarias y proporcionales?</li> </ul>
 Modificación no autorizada de los datos	<ul style="list-style-type: none"> <li>■ Ataque para la suplantación de identidad</li> <li>■ Errores en los procesos de recopilación y captura de información</li> <li>■ Modificación no autorizada de datos intencionada</li> <li>■ Uso ilegítimo de datos personales</li> </ul>	<ul style="list-style-type: none"> <li>• Existen credenciales o mecanismos de control que limiten el acceso a personal no autorizado? ¿Se revisa periódicamente la actividad realizada por los usuarios cuando acceden a los sistemas?</li> <li>• Existen controles sobre la integridad de la información durante el proceso de captura de datos? ¿Se identifica adecuadamente al interesado que proporciona los datos?</li> <li>• Los datos son modificables únicamente por el personal autorizado?</li> <li>• La actividad de tratamiento sobre los datos son acordes a las finalidades para las cuales existe una base legitimadora? ¿Se puede realizar un perfilado o una operación de tratamiento que no esté alineada con las finalidades de la operación de tratamiento?</li> </ul>
 Eliminación de los datos	<ul style="list-style-type: none"> <li>■ Corte de suministro eléctrico o fallos en servicios de comunicaciones</li> <li>■ Error humano o ataque intencionado que provoca borrado o pérdida de datos</li> <li>■ Desastres naturales</li> </ul>	<ul style="list-style-type: none"> <li>• Un fallo de suministro eléctrico puede implicar la pérdida de datos? ¿Un fallo en los servicios de comunicaciones puede ocasionar una pérdida de datos?</li> <li>• Los datos pueden ser eliminados únicamente por el personal autorizado? ¿Existen copias de seguridad?</li> <li>• Están los sistemas que almacenan datos en ubicaciones expuestas a la posibilidad de que se produzca un desastre natural? ¿Existe réplica de los datos en diferentes ubicaciones?</li> </ul>

Etapa del ciclo de vida de los datos	Amenaza identificada	Riesgo	Impacto
Ejemplo nº1	Almacenamiento de los datos	Pérdida de un dispositivo móvil o fuga de información	Vulneración de los derechos y libertades
Ejemplo nº2	Uso / tratamiento de los datos	Ataque cibernético para la suplantación de identidad	Modificación no autorizada de datos
Ejemplo nº3	Uso / tratamiento de los datos	Fallo en el suministro eléctrico o desastre natural	Borrado o pérdida de datos

rotección de datos personales

## 7.2. Riesgos

### Ejemplos de daños



Ejemplos de posibles daños físico, material o moral	
<p><b>Despreciable:</b> Los interesados no se verán prácticamente afectados o encontrarán alguna pequeña inconveniencia</p>	<ul style="list-style-type: none"> <li>■ Molestias o irritación.</li> <li>■ Se incumplen obligaciones materiales sin perjuicios relevantes.</li> <li>■ No se priva de los derechos y libertades.</li> </ul>
<p><b>Limitado:</b> Los interesados podrán encontrar inconveniencias no significativas</p>	<ul style="list-style-type: none"> <li>■ Estrés o padecimientos físicos menores.</li> <li>■ Costes extra, denegación de acceso a algunos servicios o incumplimiento de obligaciones materiales con perjuicios económicos.</li> <li>■ Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.</li> </ul>
<p><b>Significativo:</b> Los interesados encontrarán consecuencias significativas, que deberían poder superar sin dificultades serias.</p>	<ul style="list-style-type: none"> <li>■ Empeoramiento del estado de salud o agresiones físicas.</li> <li>■ Apropiación indebida de fondos, pérdida del empleo o incumplimiento de obligaciones materiales con perjuicios económicos relevantes.</li> <li>■ Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.</li> </ul>
<p><b>Máximo:</b> Los interesados encontrarán consecuencias significativas o incluso irreversibles, que podrán no llegar a superarse.</p>	<ul style="list-style-type: none"> <li>■ Agresiones físicas con consecuencias irreparables.</li> <li>■ Asunción de una deuda inafrentable, imposibilidad de volver a trabajar o incumplimiento de obligaciones materiales con perjuicios económicos irreparables.</li> <li>■ Se agrede significativamente contra los derechos y libertades de los interesados, por ejemplo, padecimiento psicológico con consecuencias a largo plazo o irreparables por la divulgación de datos sensibles.</li> </ul>

## 7.2. Riesgos

- ▶ Gestión de Riesgos por defecto: GdR
  - ▶ Requiere un profundo proceso de identificación, evaluación y tratamiento de los riesgos.
  - ▶ La metodología para la realización de una EIPD describe un proceso detallado de análisis y está enfocada a las actividades de tratamiento donde la exposición al riesgo es elevada.
    - ▶ Ante niveles de riesgo no elevados, el proceso de análisis se puede simplificar poniendo foco en aquellos más relevantes.
  - ▶ Las actividades de tratamiento donde se puede aplicar el enfoque de gestión de riesgos por defecto, analizadas previamente mediante el análisis de la necesidad de realizar una EIPD, se situarán siempre en un nivel de riesgo no elevado.

Probabilidad	Máxima 4	8	12	16
Significativa 3	3	6	9	12
Limitada 2	2	4	6	8
Despreciable 1	1	2	3	4
	Bajo Medio	Alto	Muy Alto	

Despreciable · 1   Limitada · 2   Significativa · 3   Máxima · 4

IMPACTO

## 7.2. Riesgos

- ▶ Recordemos: Riesgo = Probabilidad x Impacto



# Gestión de riesgos por defecto



Operaciones de tratamiento			
Riesgos por defecto			
Protección de los datos personales	Tipología de riesgo	Riesgos	Medidas de control
Derechos y libertades de los interesados			

## 7.2. Riesgos

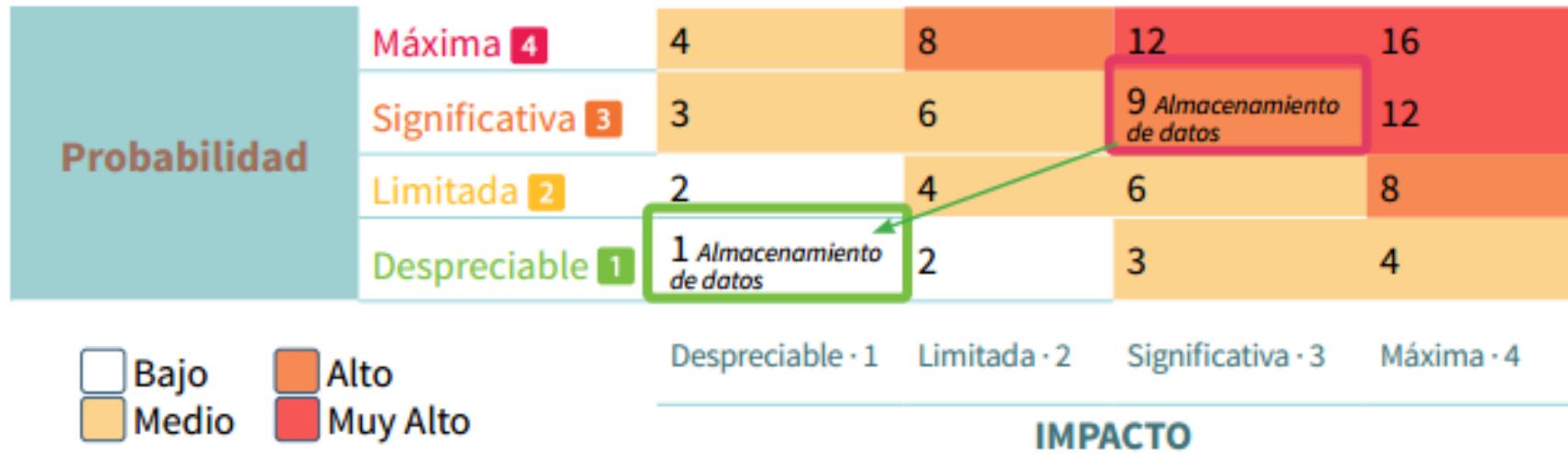
- ▶ Riesgo residual = Probabilidad X Impacto
- ▶ Ejemplo:
  - ▶ Ante un riesgo de acceso no autorizado por parte de terceros en un proceso de autenticación, el hecho de establecer un usuario y una contraseña asignados al usuario reduce significativamente la probabilidad de que un tercero pueda realizar un acceso no autorizado.
    - ▶ En este caso, la medida de control reduce la probabilidad de ocurrencia del riesgo y, por tanto, minimiza el riesgo residual asociado.
  - ▶ Ejemplo práctico de estimación del riesgo residual:
    - ▶ Ciclo de vida del dato (fase almacenamiento): Almacenamiento de datos de clientes en dispositivos móviles.
    - ▶ Amenaza: Pérdida del dispositivo móvil.
    - ▶ Riesgo: Acceso no autorizado por parte de terceros a datos de salud (violación de la confidencialidad).

## 7.2. Riesgos

- ▶ Impacto: Violación de derechos fundamentales (Significativo 3).
- ▶ Probabilidad: Se puede producir cada vez que el usuario no tiene en su poder el dispositivo móvil (Significativa 3).
- ▶ Riesgo inherente: Impacto x Probabilidad =  $3 \times 3 = 9$  (Riesgo alto).
- ▶ Medidas de control: Método de autenticación mediante usuario, contraseña y huella biométrica. Cifrado del dispositivo móvil y pseudonimización de los datos.
- ▶ Eficacia del control: Reduce la probabilidad a despreciable, debido a que, aunque se pierda el dispositivo, no será posible el acceso sin credenciales. Adicionalmente, reduce el impacto a despreciable, debido a que, aunque se pierda el dispositivo, los datos nunca serán identificables evitando producir daños sobre los interesados.
- ▶ Riesgo residual: Impacto x Probabilidad =  $1 \times 1 = 1$  (Riesgo bajo)



## 7.2. Riesgos



# 7.2. Riesgos. Normativa a contemplar



## BOLETÍN OFICIAL DEL ESTADO



Núm. 218

Sábado 8 de septiembre de 2018

Sec. I. Pág. 87675

### I. DISPOSICIONES GENERALES

#### JEFATURA DEL ESTADO

**12257** *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.*

I

La evolución de las tecnologías de la información y de la comunicación, especialmente con el desarrollo de Internet, ha hecho desempeñen actualmente un papel crucial seguridad aspectos esenciales para el desarrollo social.

Por ello, los incidentes que, al afectar a dichas actividades, representan una grave amenaza y provienen de acciones deliberadas pueden erosionar la confianza de la población y, en definitiva,

19.7.2016

ES

Diario Oficial de la Unión Europea

L 194/1

I

(Actos legislativos)

#### DIRECTIVAS

##### DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 6 de julio de 2016

relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

# 7.2. Riesgos. Normativa a contemplar



## Guía de Seguridad de las TIC CCN-STIC 817

### ESQUEMA NACIONAL DE SEGURIDAD GESTIÓN DE CIBERINCIDENTES



Junio 2018



## BOLETÍN OFICIAL DEL ESTADO

Núm. 121

Sábado 21 de mayo de 2011

Sec. I. Pág. 50808



### I. DISPOSICIONES GENERALES

#### MINISTERIO DEL INTERIOR

**8849** *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.*

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas habilita al Gobierno, en su disposición final cuarta, para dictar el Real decreto de ejecución de desarrollo de la mencionada Ley.



### LEGISLACIÓN CONSOLIDADA

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Jefatura del Estado  
«BOE» núm. 102, de 29 de abril de 2011  
Referencia: BOE-A-2011-7630

### TEXTO CONSOLIDADO

Última modificación: sin modificaciones