



BABEL

We partner to woow



FORMACIÓN BÁSICA EN MATERIA DE PROTECCIÓN DE DATOS Y PRIVACIDAD

Una visión práctica





índice

1. Normatividad
2. Principales conceptos
3. Principios rectores
4. Medidas de seguridad
5. Cuestiones prácticas
6. Dudas y consultas



ANTECEDENTES CONSTITUCIONALES

Artículo 18 (C.E.)

- Derecho al **honor y propia imagen**
- Inviolabilidad del **domicilio**
- **Secreto** de las comunicaciones

Legislación consolidada



Constitución Española.

Publicado en: «BOE» núm. 311, de 29/12/1978.
 Entrada en vigor: 29/12/1978
 Departamento: Cortes Generales
 Referencia: [BOE-A-1978-31229](#)
 Permalink ELI: [https://www.boe.es/eli/es/c/1978/12/27/\(1\)/con](https://www.boe.es/eli/es/c/1978/12/27/(1)/con)

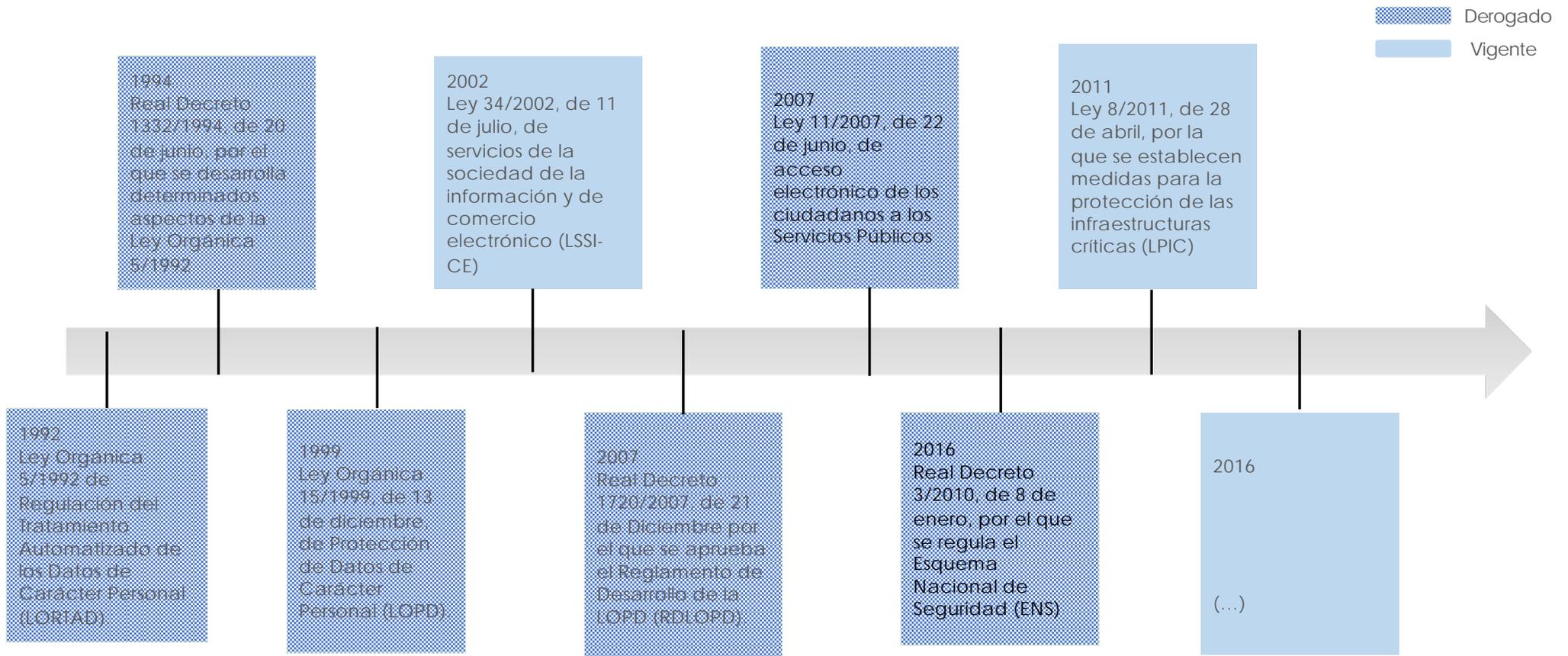
Autodeterminación informativa

4 idiomas ▼

[Artículo](#) [Discusión](#)
[Leer](#) [Editar](#) [Ver historial](#) [Herramientas](#) ▼

La **autodeterminación informativa** es un **derecho fundamental** derivado del derecho a la privacidad, que se concreta en la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en **registros** públicos o privados, especialmente -pero no exclusivamente- los almacenados en medios **informáticos**. El derecho sustantivo a la autodeterminación informativa se ve complementado, en el plano **procesal**, por el llamado recurso de **habeas data**.¹

ANTECEDENTES NORMATIVOS



Reglamento 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a su libre circulación

Ley Orgánica 3/2018 de Protección de Datos (LOPD)
y Garantía de los Derechos Digitales (GDD)

EUROPEA

NACIONAL

INSTRUCCIONES



RESOLUCIONES



NORMATIVA
SECTORIAL

SENTENCIAS
TRIBUNALES



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



Buscar...

Buscar

Sede elec

Inicio La Agencia ▾ Derechos y deberes ▾ Áreas de actuación ▾ Publicaciones y resoluciones Intern

Circular sobre el derecho de los usuarios a no recibir llamadas comerciales no solicitadas

El documento fija los criterios conforme a los que va a actuar la Agencia en aplicación del artículo 66.1 b) de la Ley General de Telecomunicaciones, que implica cambios sustanciales para poder realizar este tipo de llamadas y que se aplica desde el 29 de junio

ACCESO A LA CIRCULAR



<https://edpb.europa.eu/>

European Data Protection Board



European Data Protection Board



BINDING DECISIONS

DICTÁMENES

GUIDANCE

CONSULTA PÚBLICA

REGISTERS



DATA PROTECTION GUIDE FOR SMALL BUSINESS

BABEL

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos



EUROPEAN DATA
PROTECTION SUPERVISOR

The European guardian of personal data protection

01110101110111011
011101111



apdcat

Autoritat Catalana de Protecció de Dades



Consejo de Transparencia
y Protección de Datos
de Andalucía



índice

1. Normatividad
2. Principales conceptos
3. Principios rectores
4. Medidas de seguridad
5. Cuestiones prácticas
6. Dudas y consultas



DATOS DE CARÁCTER PERSONAL

“toda información sobre una persona física identificada o identificable”

“se considerará persona física identificable 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”



TIPOLOGÍA DE DATOS

Datos particularmente sensibles (Países miembro)

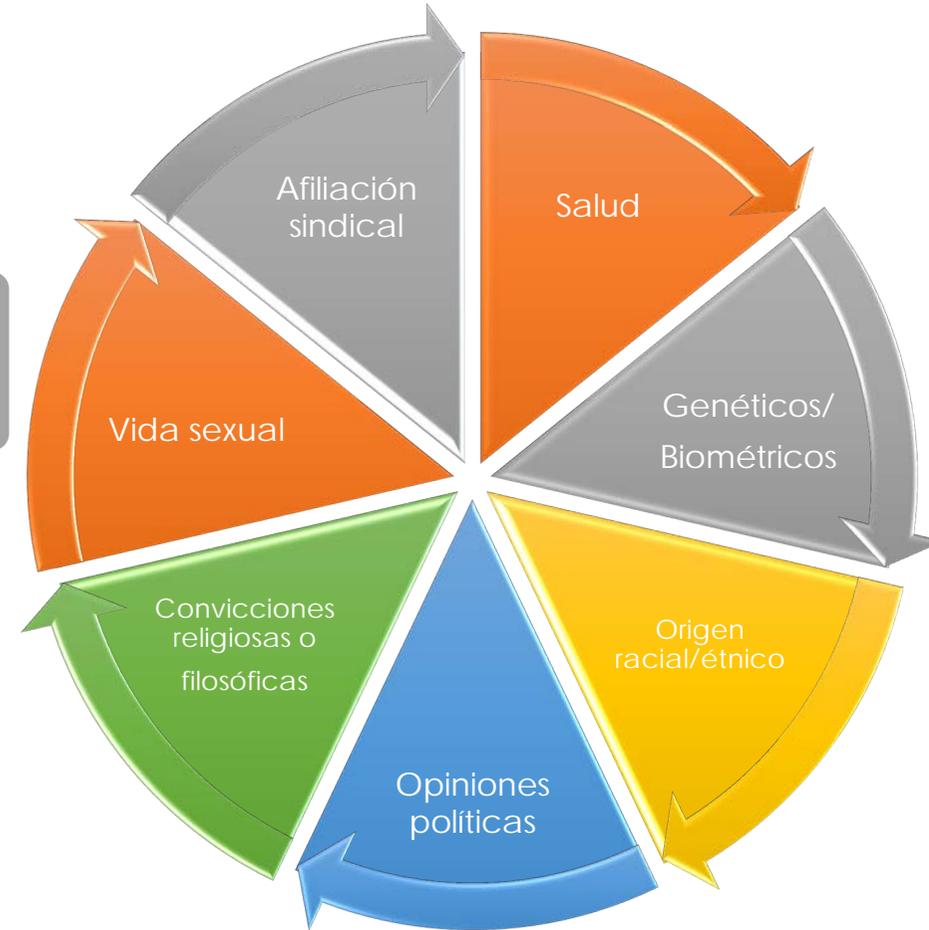
Aquellos, cuyo tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales

Considerando
51

LOPDgdd

- Infracciones administrativas/penales
- Víctimas de violencia de género

Datos especialmente protegidos (Artículo 9)



RESPONSABLE DEL TRATAMIENTO



El “responsable del tratamiento” o “responsable” es 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 DEL TRATAMIENTO

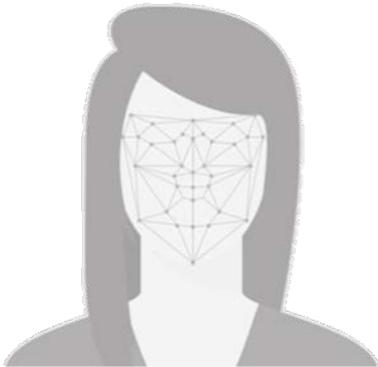
Es la persona física o jurídica, autoridad pública, servicio u otro organismo que **trate datos por cuenta del responsable del tratamiento.**

EJEMPLOS

- La elaboración de las nóminas
- La destrucción de documentación
- Profesores externos
- Proveedor de plataforma e-learning



INTERESADO Y TRATAMIENTO



- Nombre
- Apellidos
- Fecha de nacimiento
- Residencia
- DNI
- Matricula
- Huella Dactilar
- Dirección IP
- ...

Datos personales

Información relativa a una persona física, que nos puede permitir determinar directa o indirectamente su identidad



Interesado/**afectado**

Persona física sometida al tratamiento de sus datos personales

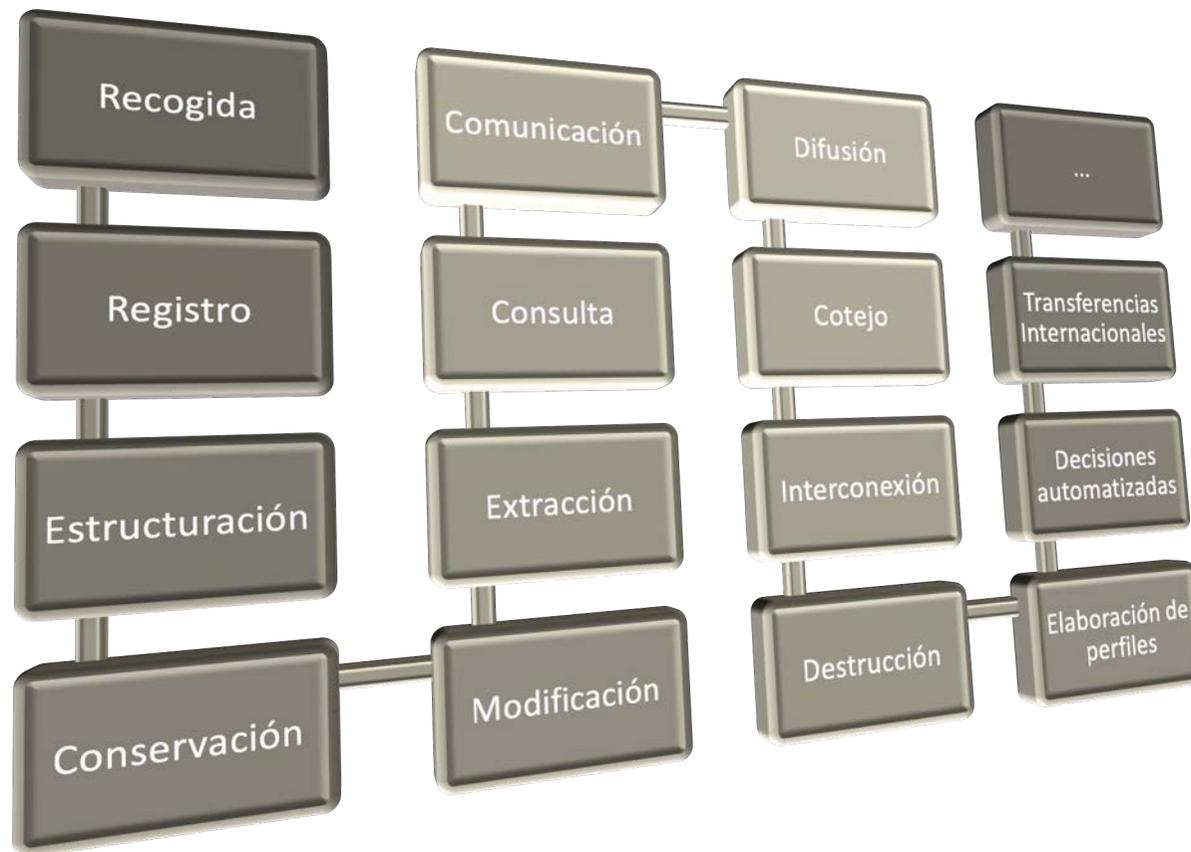


Tratamiento



Tratamiento

Operaciones que se realizan sobre los datos personales



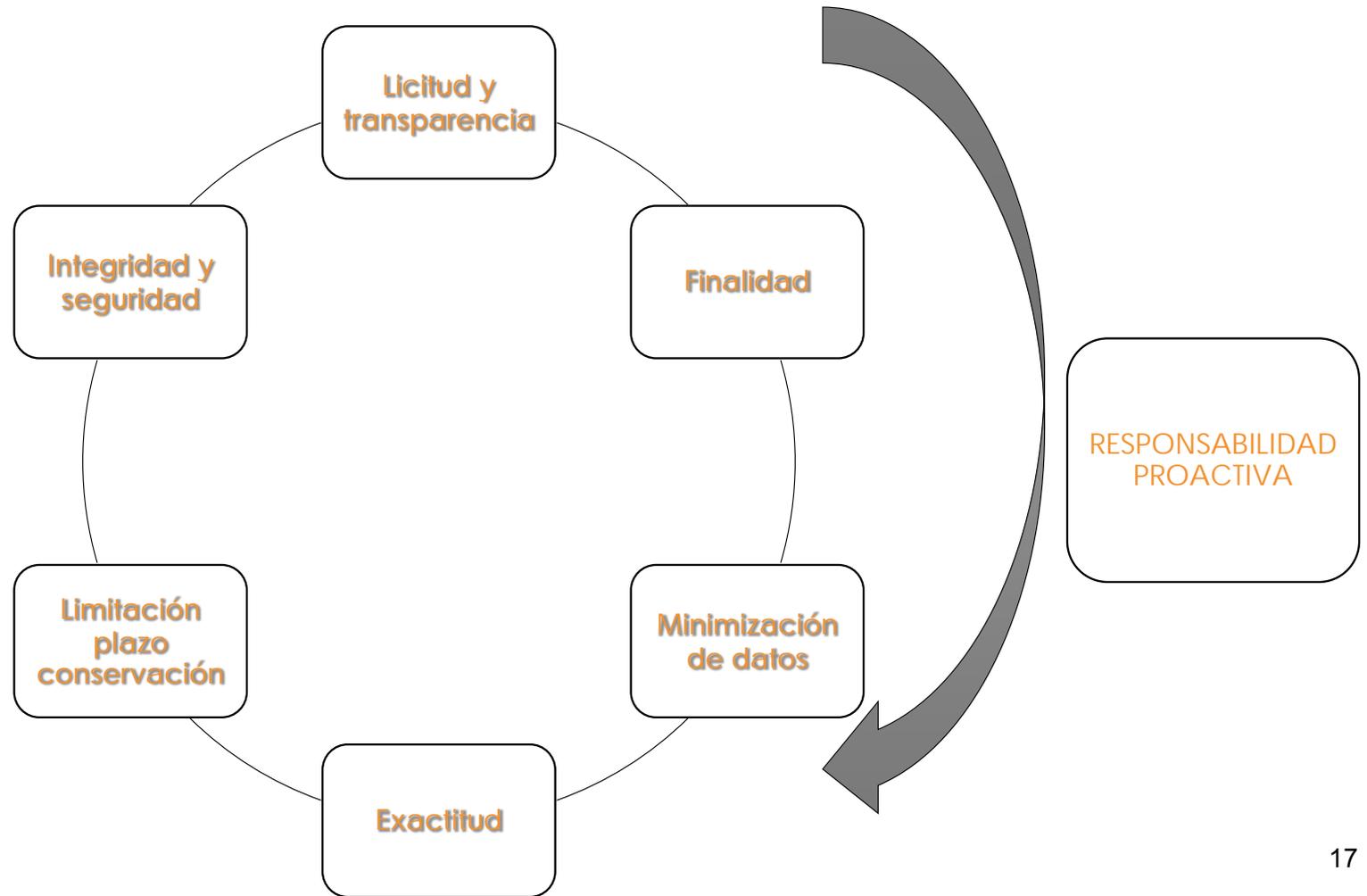


índice

1. Normatividad
2. Principales conceptos
3. Principios rectores
4. Medidas de seguridad
5. Cuestiones prácticas
6. Dudas y consultas



PRINCIPIOS RECTORES



Licitud y
transparencia



El interesado de su **consentimiento**



Necesario para la ejecución de un **contrato**



Necesario para el cumplimiento de una **obligación legal**



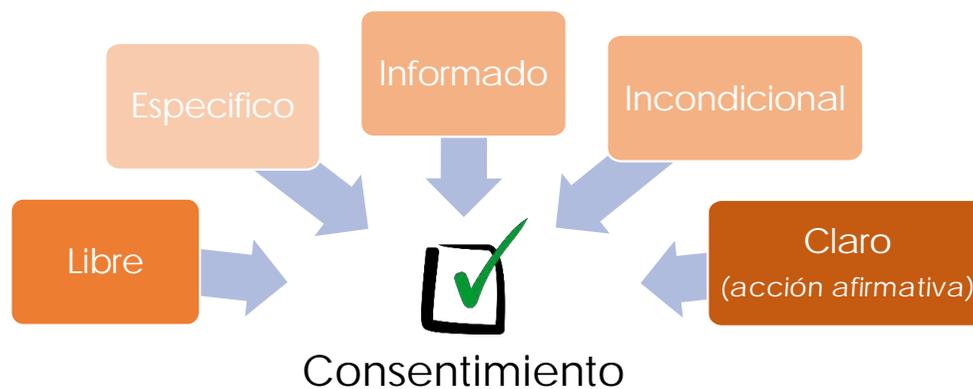
Necesario para proteger **interés vital** del interesado



Cumplimiento de una misión de **interés público**



Necesario para satisfacer el **interés legítimo** del Responsable del Tratamiento



 Marcar una casilla

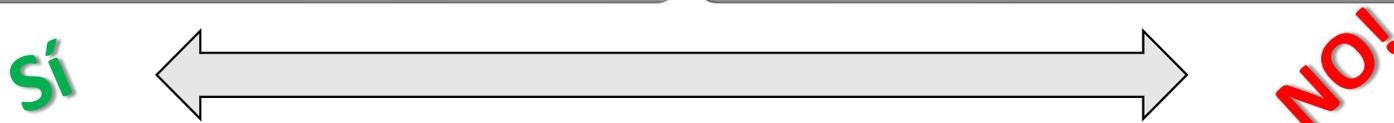
 Casillas premarcadas

 Escoger parámetros técnicos

 Silencio

 Otra declaración o comportamiento

 Inacción



PRINCIPIOS RECTORES

Finalidad

obligación de que los datos sean tratados con una o varias finalidades **determinadas, explícitas y legítimas**

se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos **sean tratados posteriormente de una manera incompatible con esos fines.**



Minimización de datos

Los datos personales serán **adecuados, pertinentes y limitados a lo necesario** en relación con los fines para los que son tratados.

No es posible recabar y tratar datos simplemente “por tenerlos”



PRINCIPIOS RECTORES

Exactitud

Los datos personales serán **exactos y si fuera necesario actualizados**, adoptándose medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos respecto a los fines para los que se tratan



Limitación del plazo de conservación

Los datos no podrán ser mantenidos por mas tiempo del necesario para los fines del tratamiento.

Superado este tiempo, tan solo podría conservarse con las finalidades de archivo en interés público, fines de investigación científica o histórica o fines estadísticos



Integridad y
seguridad

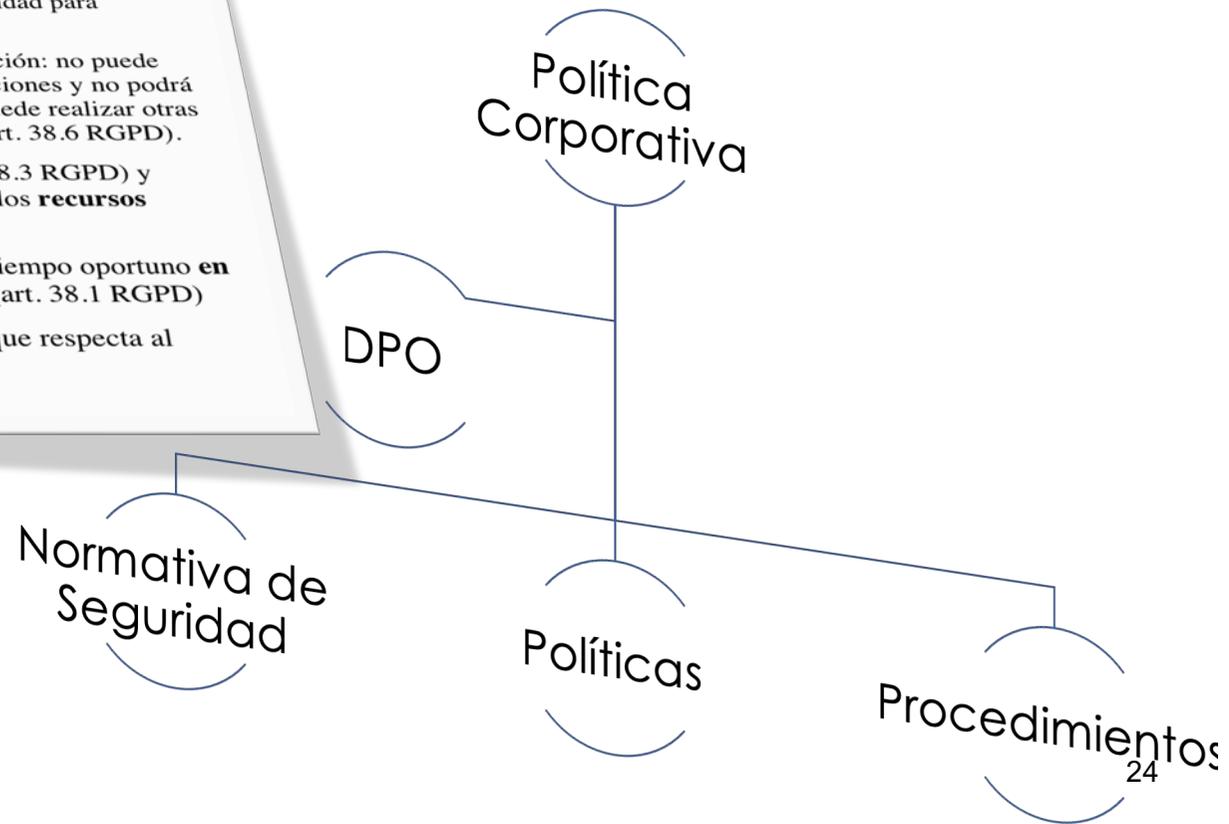
“Teniendo en cuenta el tratamiento (...), así como los riesgos de diversa probabilidad y gravedad, el responsable del tratamiento **aplicará medidas técnicas y organizativas apropiadas**”



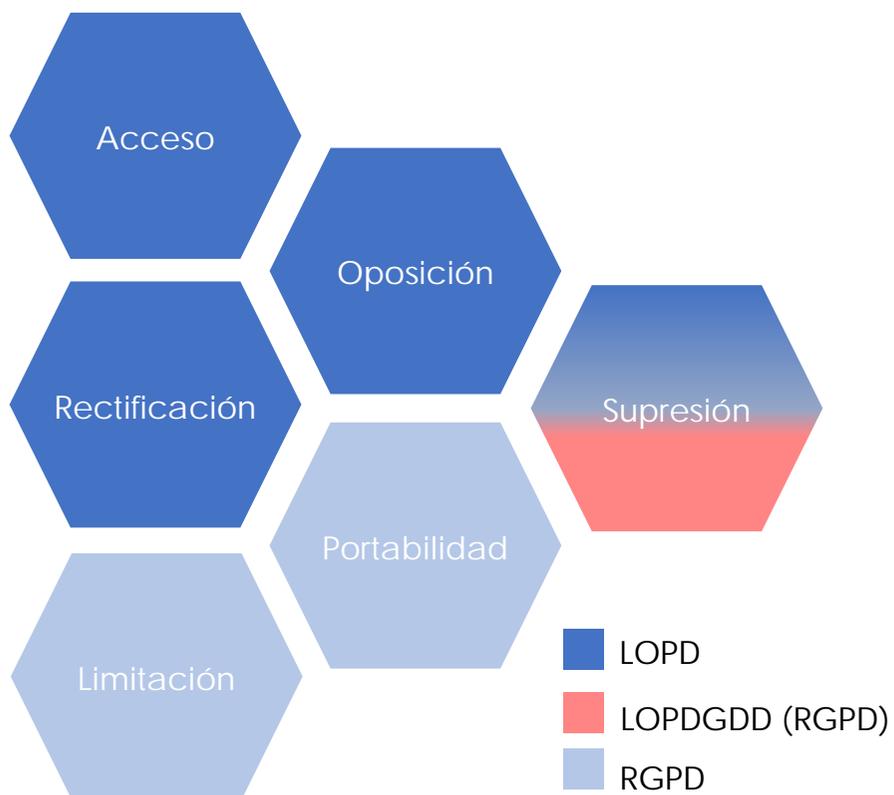


Estatuto jurídico del DPD

- ◆ El nombramiento de un DPD es **obligatorio** en determinados supuestos determinados en el RGPD y en la LOPDGDD, entre los que se encuentran las **Fundaciones del sector público**.
- ◆ De acuerdo con lo dispuesto en el art. 37.1 RGPD será designado atendiendo a “sus cualidades profesionales y, en particular, a sus **conocimientos especializados del Derecho y la práctica en materia de protección de datos** y a su capacidad para desempeñar las funciones indicadas en el art. 39.”
- ◆ Se le garantiza una **posición de independencia** dentro de la organización: no puede recibir ninguna instrucción en lo que respecta al desempeño de sus funciones y no podrá ser sancionado ni destituido por cumplir con ellas (art. 38.3 RGPD). Puede realizar otras tareas y cometidos siempre que no den lugar a conflicto de intereses (art. 38.6 RGPD).
- ◆ **Rendirá cuentas directamente al más alto nivel jerárquico** (art. 38.3 RGPD) y deberá ser **respaldado en el ejercicio de sus funciones**, facilitándole los **recursos necesarios** para ello (art. 38.2 RGPD).
- ◆ Se deberá **garantizar su participación** en la forma adecuada y en tiempo oportuno en **todas las cuestiones relativas a la protección de datos personales** (art. 38.1 RGPD)
- ◆ Está **obligado a mantener el secreto o la confidencialidad** en lo que respecta al desempeño de sus funciones. (art. 38.5 RGPD).

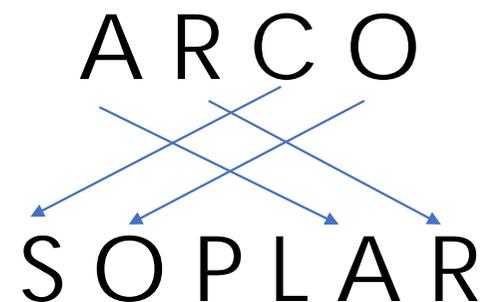


DERECHOS DE LOS AFECTADOS



Con el cambio al reglamento se introducen tres nuevos derechos

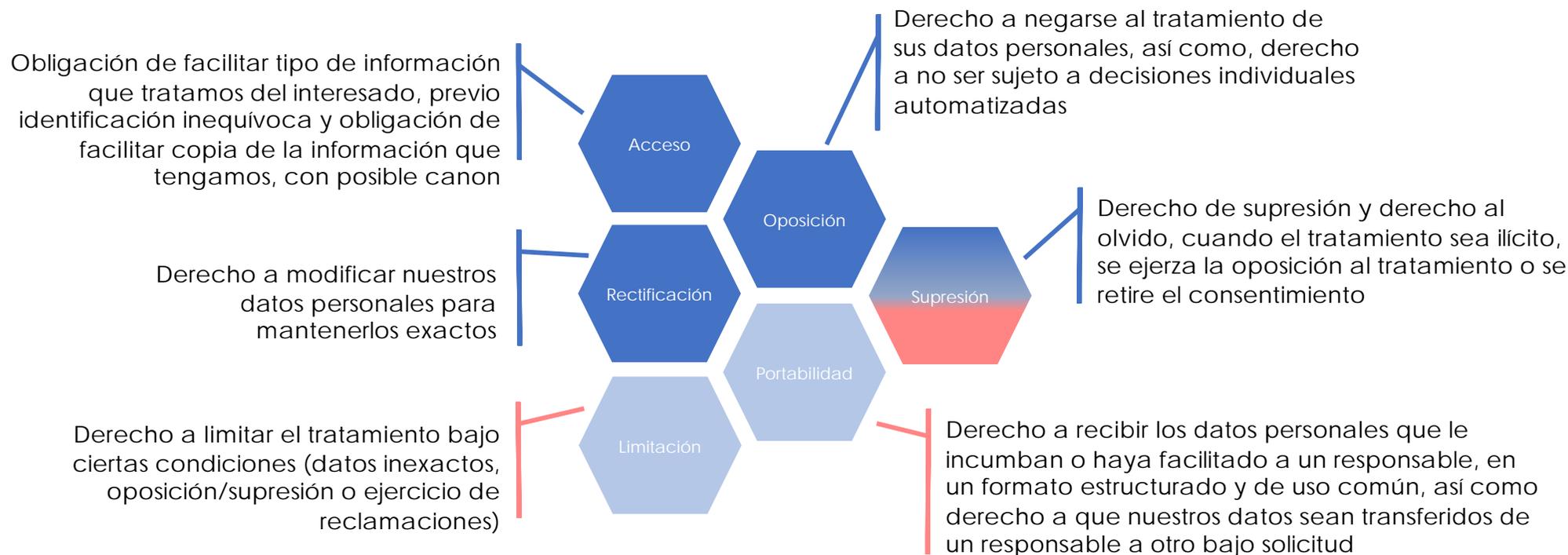
A R C O
S O P L A R



The diagram shows the mnemonic 'ARCO SOPLAR' with blue arrows connecting the letters. The 'A' connects to 'S', 'R' to 'O', 'C' to 'P', and 'O' to 'L'. The 'S', 'O', 'P', and 'L' are grouped together, representing the new rights introduced by the regulation.

No esta comprendido como un derecho, pero se trata de una obligación de la organización, la de informar al interesado que puede presentar una reclamación ante la Autoridad de Control

DERECHOS DE LOS AFECTADOS





índice

1. Normatividad
2. Principales conceptos
3. Principios rectores
4. Medidas de seguridad
5. Cuestiones prácticas
6. Dudas y consultas



MEDIDAS DE SEGURIDAD

Disposición adicional 1ª LOPDGDD

75 MEDIDAS DE SEGURIDAD RECOGIDAS EN EL ENS

MARCO ORGANIZATIVO

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad

4

POLÍTICA DE SEGURIDAD
NORMATIVA DE SEGURIDAD
PROCEDIMIENTOS DE SEGURIDAD
PROCESO DE AUTORIZACIÓN

MARCO OPERACIONAL

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin

31

PLANIFICACIÓN
CONTROL DE ACCESO
EXPLOTACIÓN
SERVICIOS EXTERNOS
CONTINUIDAD DEL SERVICIO
MONITORIZACIÓN DEL SISTEMA

MEDIDAS DE PROTECCIÓN

Las medidas de protección, se centrarán en activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad

40

INSTALACIONES E INFRAESTRUCTURAS
GESTIÓN DEL PERSONAL
PROTECCIÓN DE LOS EQUIPOS
PROTECCIÓN DE LAS COMUNICACIONES
PROTECCIÓN SOPORTES DE INFORMACIÓN
PROTECCIÓN APLICACIONES INFORMÁTICAS
PROTECCIÓN DE LA INFORMACIÓN
PROTECCIÓN DE LOS SERVICIOS

Valoración de los sistemas



Relación entre ENS y RGPD/LOPDGDD

ASPECTO	ESQUEMA NACIONAL DE SEGURIDAD	RGPD/LOPDGDD
Análisis de riesgos	<p>Artículo 7. Gestión de la seguridad basada en los riesgos</p> <p>Artículo 14. Análisis y gestión de los riesgos.</p> <p>Medida - Anexo II.op.pl.1. Análisis de riesgos.</p>	Artículo 32. Seguridad del tratamiento.
Activos (inventario)	Elementos que constituyen el sistema de información (software, hardware, comunicaciones...)	Tratamientos de datos personales.
Planes de acción	Plan de Tratamiento de riesgos + plan de cumplimiento = Plan de Mejora de la Seguridad.	Plan de Tratamiento de riesgos + plan de cumplimiento jurídico = Plan de Cumplimiento RGPD.
Documentación	<p>Análisis de riesgo y Planes de Seguridad, Política, Normativas, Procedimientos.</p> <p>Registros de cumplimiento (evidencias)</p>	<p>Análisis de riesgo y Planes de Seguridad, Manual de procedimientos jurídicos, políticas del encargado o responsable.</p> <p>Registros de cumplimiento (evidencias)</p>

Relación entre ENS y RGPD/LOPDGDD

ASPECTO	ESQUEMA NACIONAL DE SEGURIDAD	RGPD/LOPDGDD
Incidentes/ Violaciones	<p>Artículo 25. Incidentes de seguridad.</p> <p>Medida - Anexo II. op.exp.7. Gestión de incidentes.</p> <p>Medida - Anexo II. op.exp.9. Registro de la gestión de incidentes.</p>	<p>Violación de la seguridad de los datos personales.</p> <p>Artículo 33 Notificación de una violación de la seguridad de los datos personales a la autoridad de control.</p> <p>Artículo 34 Comunicación de una violación de la seguridad de los datos personales al interesado.</p>
Protección de datos desde el diseño y por defecto	<p>Artículo 19. Mínimo privilegio.</p> <p>Medida - Anexo II. op.pl.3. Adquisición de nuevos componentes</p> <p>Medida - Anexo II. mp.sw.1. Desarrollo de aplicaciones.</p>	<p>Artículo 25 Protección de datos desde el diseño y por defecto.</p>

Relación entre ENS y RGPD/LOPDGDD

ASPECTO	ESQUEMA NACIONAL DE SEGURIDAD	RGPD/LOPDGDD
Roles y responsabilidades	<p>Responsable de seguridad</p> <p>Responsable de la información y servicio</p> <p>Responsable del Sistema</p>	<p>DPO</p> <p>Responsable de tratamiento</p> <p>Encargado de tratamiento</p>
Gestion de terceros	op.ext. Servicios externos	Artículo 28 Encargado del tratamiento
Auditoría	<p>Artículo 31. Auditoría de la seguridad.</p> <p>Anexo III. Auditoría de la Seguridad</p>	<p>Artículo 39. Funciones del DPO</p> <p>1.b) supervisar las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales incluida las auditorías correspondientes.</p> <p>Artículo 24 del RGPD. Responsabilidad del responsable del tratamiento. Apartado 1 "Dichas medidas se revisarán y actualizarán cuando sea necesario".</p>

Relación entre ENS y RGPD/LOPDGDD

ASPECTO	ESQUEMA NACIONAL DE SEGURIDAD	RGPD/LOPDGDD
Formación y concienciación	<p>Artículo 16. Profesionalidad.</p> <p>Medida - Anexo II. mp.per.3. Concienciación</p> <p>Medida - Anexo II. mp.per.4. Formación</p> <p>Disposición adicional primera. Formación.</p>	<p>Artículo 39. Funciones del DPO</p> <p>1.b) supervisar las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la concienciación y formación del personal que participa en las operaciones de tratamiento.</p>
Indicadores	<p>Artículo 32. Informe de Estado de la Seguridad (INES)</p> <p>Medida - Anexo II.op.mon.2. Sistema de Métricas</p>	<p>Artículo 39. Funciones del DPO</p> <p>1.b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento – Los resultados de esta supervisión deberían ser evaluados (cuantificados).</p>

Riesgos de seguridad de la información y privacidad

Acciones	Compliance
Técnicas y organizativas	ENS (anexo II)
Jurídicas	RGPD/LOPDGDD

Mitigación de riesgos de seguridad y privacidad



EVALUACIONES DE IMPACTO



72 HORAS



BRECHAS DE SEGURIDAD

Roj: STS 543/2022 - ECLI:ES:TS:2022:543

Id Cendoj: 28079130032022100030

Órgano: Tribunal Supremo. Sala de lo Contencioso

Sede: Madrid

Sección: 3

Fecha: 15/02/2022

Nº de Recurso: 7359/2020

Nº de Resolución: 188/2022

Procedimiento: Recurso de Casación Contencioso-Administrativo (L.O. 7/2015)

Ponente: DIEGO CORDOBA CASTROVERDE

Tipo de Resolución: Sentencia

Resoluciones del caso: SAN 2207/2020,
ATS 4672/2021,
STS 543/2022

Obligación de medios

Indica el Tribunal Supremo que tan solo resulta exigible a los responsables y encargados del tratamiento la adopción e implantación de medidas técnicas y organizativas que, *conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión*, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado.



índice

1. Normatividad
2. Principales conceptos
3. Principios rectores
4. Medidas de seguridad
5. Cuestiones prácticas
6. Dudas y consultas



Licitud y
transparencia



¿Se pueden recabar datos sobre la situación familiar de los padres de los alumnos?

Sí, los centros educativos pueden recabar la información sobre la situación familiar de los alumnos. Esta información debe estar actualizada y los progenitores han de informar a los centros sobre cualquier modificación.

Si los padres del alumno están separados o divorciados, debe recabarse información sobre quién ostenta la patria potestad, si ambos o uno sólo, y quién ostenta la guarda y custodia. También de quiénes son las personas autorizadas a recoger al alumno.



¿Se pueden recabar datos de salud?

Sí, en la medida en que sean necesarios para el ejercicio de la función educativa. Se pueden distinguir los siguientes momentos:

- En la matriculación del alumno: discapacidades, enfermedades crónicas, TDAH, intolerancias alimentarias o alergias.
- Durante el curso escolar: el tratamiento médico que reciba un alumno a través del servicio médico o de enfermería del centro o los informes de centros sanitarios a los que se le haya trasladado como consecuencia de accidentes o indisposiciones sufridas en el centro o los informes de los equipos de orientación psicopedagógica.

Finalidad

Minimización de datos



¿Se pueden recabar imágenes de los alumnos para el expediente académico?

Entre los datos que pueden recabar los centros educativos para el ejercicio de la función docente y orientadora sin consentimiento de los alumnos se pueden incluir sus fotografías a los efectos de identificar a cada alumno en relación con su expediente.



¿Se pueden recabar datos para finalidades distintas de la función propiamente educativa?

Al margen de la función educativa, los centros pueden recabar datos para otras finalidades legítimas, como puede ser la gestión de la relación jurídica derivada de la matriculación de los alumnos, o dar a conocer la oferta académica, participar con los alumnos en concursos educativos u ofrecer servicios deportivos, de ocio o culturales. En estos casos, se podrán recabar bien como consecuencia de la relación jurídica establecida con la matrícula o si media el consentimiento previo de los alumnos o de sus padres o tutores.

Además, con carácter previo a la obtención del consentimiento, se debe cumplir con el derecho de información de los titulares de los datos o a sus padres o tutores si son menores de 14 años, como se especifica en el apartado II.c) sobre Transparencia e información.

Finalidad



¿Puede un centro dar publicidad a las listas de alumnos admitidos?

Sí. El centro necesita informar sobre los alumnos que han sido admitidos en la medida en que la admisión se realiza mediante un procedimiento de concurrencia competitiva en el que se valoran y puntúan determinadas circunstancias.

No obstante, la publicidad deberá realizarse de manera que no suponga un acceso indiscriminado a la información, por ejemplo, publicando la relación de alumnos admitidos en los tablones de anuncios en el interior del centro o en una página web de acceso restringido a quienes hayan solicitado la admisión.

Esta publicación deberá recoger sólo el resultado final del baremo, no resultados parciales que puedan responder a datos o información sensible o poner de manifiesto la capacidad económica de la familia.

Esta información, no obstante, estará disponible para los interesados que ejerciten su derecho a reclamar.

Cuando ya no sean necesarios estos listados, hay que retirarlos, sin perjuicio de su conservación por el centro a fin de atender las reclamaciones que pudieran plantearse.

Alumno	Matemáticas	Lengua	Historia	Música
Alberto Pérez	9	8	7	7
Antonio Domingo	6	5	5	6
Carlos López	7	7	8	7
Carolina Sánchez	6	4	5	7
Media	7	6	6.25	6.75
Suspensos	0	1	0	0
probados	4	3	4	4



¿Pueden los centros hacer públicas las relaciones de los beneficiarios de becas, subvenciones y otras ayudas públicas?

La Ley de Transparencia y Acceso a la Información Pública y Buen Gobierno determina la obligación de hacer pública, como mínimo, la información relativa a las subvenciones y ayudas públicas concedidas por las Administraciones públicas con indicación de su importe, objetivo o finalidad y los beneficiarios.

Sin perjuicio de la publicación por parte de la Administración convocante, los centros escolares también podrán publicar esta información a efectos informativos de los afectados.

A título general, en ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente, como mucho, se publicará el nombre, apellidos y 4 cifras de DNI de manera aleatoria.

Licitud y
transparencia

CRITERIOS DE PUBLICACIÓN

DISPOSICIÓN ADICIONAL 7ª LOPDGDD

El procedimiento para la determinación de forma aleatoria de las cuatro cifras numéricas a publicar del código de identificación de un interesado se realizó mediante el **proceso de selección aleatoria en una bolsa opaca de una bola de entre cinco bolas numeradas del 1 al 5**, realizado el 27 de febrero de 2019 en la AEPD.



Integridad y
seguridad

d.i Utilización de plataformas educativas

Las implicaciones que en materia de protección de datos plantea el uso de plataformas educativas, tanto de gestión como de aprendizaje o entornos virtuales de aprendizaje, se recogen en el citado Informe de la Inspección sectorial sobre el uso de servicios de *cloud computing* en el sector educativo, que incluye las recomendaciones a aplicar por los centros o las Administraciones educativas y que se aconseja consultar.

- *Se pretende constituir un grupo de WhatsApp en el que participen los delegados y los estudiantes*

Se requiere el consentimiento de cada uno de los que vayan a participar o unirse al grupo ya creado, al no entrar este supuesto en las restantes bases jurídicas de legitimación del tratamiento. No existe un interés público en que cada persona participante conozca los teléfonos del resto.



Buena práctica: resulta recomendable, como se ha indicado en el epígrafe de “estudiantes”, que la comunicación entre delegados y estudiantes, siempre que los primeros actúen en el desempeño de sus funciones, se realice mediante medios técnicos establecidos por la Universidad (por ejemplo, a través de una lista de distribución).



- *Creación de grupos entre profesores y estudiantes con aplicaciones de mensajería instantánea*

Se requiere el consentimiento de cada uno de los que vayan a participar en el grupo, al no entrar este supuesto en las restantes bases jurídicas de legitimación del tratamiento.



Buena práctica: resulta recomendable que se empleen los medios técnicos establecidos por la Universidad (por ejemplo, uso de plataformas institucionales de apoyo a la docencia o listas de distribución).





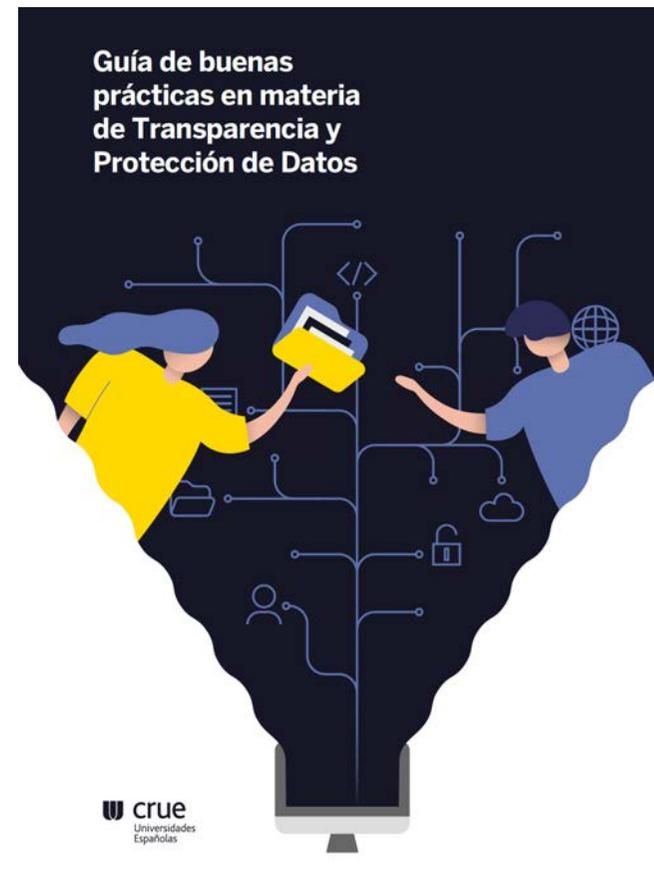
¿Se pueden instalar cámaras de videovigilancia en todas las instalaciones del colegio?

Limitación del
plazo de
conservación

No en todas las instalaciones. Dada la intromisión que supone en la intimidad de las personas, tanto de los alumnos como de profesores y demás personas cuya imagen puede ser captada por las cámaras, los sistemas de videovigilancia no podrán instalarse en aseos, vestuarios o zonas de descanso de personal docente o de otros trabajadores.



GUÍA DE RECURSOS



GUÍA DE RECURSOS

Guías

- AEPD:
 - ✓ [Guía centros educativos](#)
- CRUE
 - ✓ [Guía en el ámbito universitario en tiempos del COVID-19](#)
 - ✓ [Guía de buenas prácticas y transparencia](#)

Informes

- ✓ [Informe 36/2019](#)



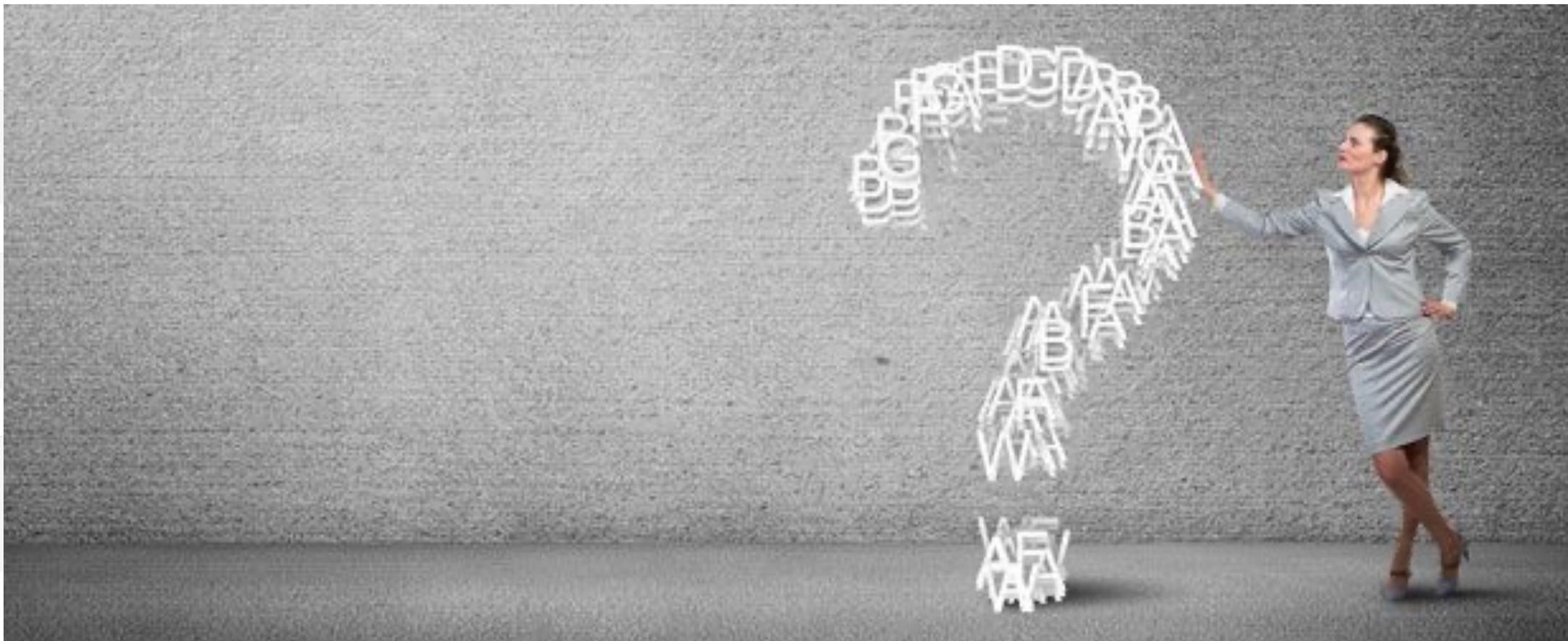
índice

1. Normatividad
2. Principales conceptos
3. Principios rectores
4. Medidas de seguridad
5. Cuestiones prácticas
6. Dudas y consultas





Dudas y consultas





España

Avilés
Barcelona
Madrid
Málaga
Sevilla

Portugal

Lisboa
Proença-a-Nova

Chile

Santiago de Chile

EEUU

New Haven

México

Ciudad de México

www.babelgroup.com

