



BABEL



**FUNDACIÓN
COMPLUTENSE**

**Implicaciones del RGPD
en el ENS**

Índice

Introducción

- Antecedentes
- Actualidad
- Regulaciones
- Principales conceptos

Figuras principales en el RGPD

- Roles y responsabilidades

Principios rectores

- Licitud y transparencia
- Finalidad
- Minimización de datos
- Exactitud
- Limitación del plazo de conservación
- Integridad y seguridad
- Responsabilidad proactiva

Obligaciones de responsables y encargados del tratamiento

- Normativa de Gestión de la clasificación y tratamiento de la Información
- Obligaciones de responsables y encargados del tratamiento
- Seguridad en la relación con proveedores
- Legitimación para el tratamiento
- Deber de información
- Transferencias internacionales

Registro de las actividades del tratamiento (RAT)

Derechos de los afectados

Proveedores

Controles y medidas de seguridad

- Protección de datos desde el diseño y por defecto
- Medidas de seguridad

Detección y reacción frente a brechas de seguridad

Evaluación de impacto

Autoridades de control

Infracciones y sanciones

LOPD. Garantía de los Derechos Digitales

Buenas Prácticas

Conclusiones





Introducción

Nociones y definiciones básicas

Constitución Española 1978

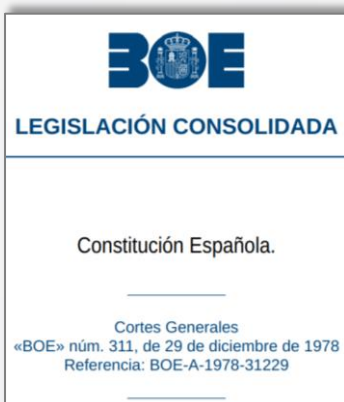
Artículo 18 de la Constitución: derecho al honor, a la intimidad personal y familiar y a la propia imagen.



Proporciona el fundamento constitucional para la protección de datos en España.



Derecho fundamental a la protección de datos, reviste forma de Ley Orgánica



Artículo 18

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
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

1992
Ley Orgánica 5/1992
De Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

2002
Ley 34/2002
De servicios de la sociedad de la información y de comercio electrónico (LSSI-CE)

2007
Ley 11/2007
De acceso electrónico de los ciudadanos a los Servicios Públicos
RD 1720/2007
Desarrolla la Ley Orgánica 15/1999 y las disposiciones relativas al ejercicio de la AEPD

2010
RD 3/2010
Se regula el Esquema Nacional de Seguridad (ENS)

1994
RD 1332/1994
Se desarrollan aspectos de la Ley Orgánica 5/1992

1999
Ley Orgánica 15/1999
De Protección de Datos de Carácter Personal (LOPD).
RD 994/1999
Medidas de seguridad de ficheros automatizados con datos de carácter personal.

2011
Ley 8/2011
Se establecen medidas para la protección de las infraestructuras críticas (LPIC)


Actualidad

VIGENTE DEROGADO



RGPD

Reglamento (UE) 2016/679

Establece las normas de protección de datos personales, su tratamiento y libre circulación en la UE.



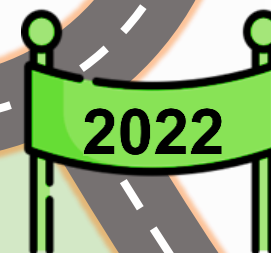
LOPD

Ley Orgánica 3/2018

Adapta el ordenamiento jurídico español al RGPD y garantiza el derecho fundamental de los españoles a la protección de los datos personales.



La disposición adicional primera LOPDGDD prescribe la implantación de las medidas del ENS al sector público.



ENS

RD 311/2022

Última versión del Esquema Nacional de Seguridad.

VIGENTE DEROGADO

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 y Garantía de los Derechos Digitales

Instrucciones y Guías de la AEPD

Resoluciones de la AEPD

Normativa sectorial

Sentencias tribunales

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Guías del CCN

Herramientas CCN

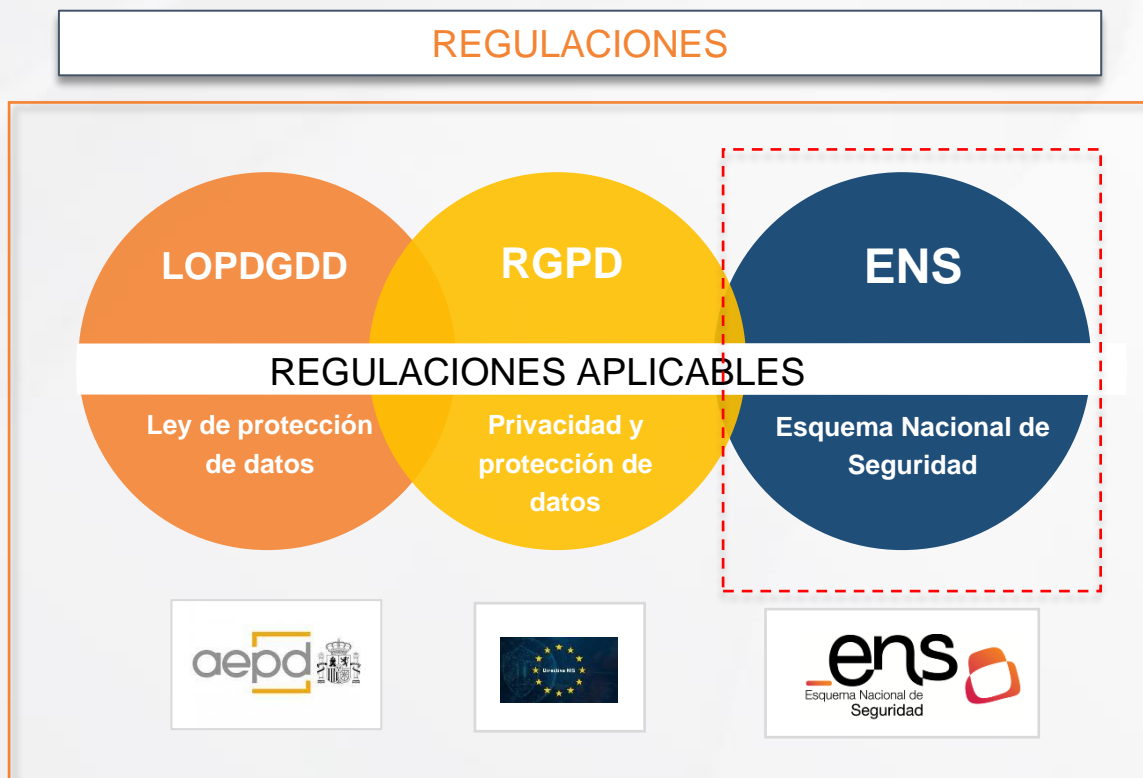
EUROPEA

NACIONAL

Regulaciones - Estándares

FGUCM en el desarrollo de sus funciones **está alineada y da cumplimiento a diversas regulaciones y estándares de buenas prácticas en materia de seguridad de la información.**

En la siguiente ilustración se muestran algunas regulaciones y estándares:



Estándares y buenas prácticas





Datos personales

“Toda información sobre una persona física **identificada o identificable**”.



Persona física identificada o identificable

Toda persona cuya **identidad pueda determinarse** directa o indirectamente, en mediante un identificador, como un nombre, datos de localización, imagen, voz, etc.



Tratamiento

Operación o conjunto de **operaciones** realizadas sobre datos personales, ya sea por procedimientos automatizados o no.



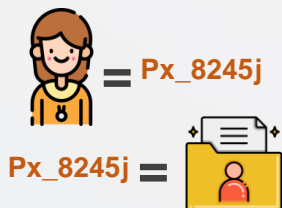
Ejemplos de tratamiento:

- La elaboración de las nóminas.
- La destrucción de documentación.
- El control de las cámaras de videovigilancia.
- Gestión del cobro de impuestos.
- Mantenimiento de los equipos informáticos.



Limitación del tratamiento

Restricción el uso de los datos para ciertos fines.



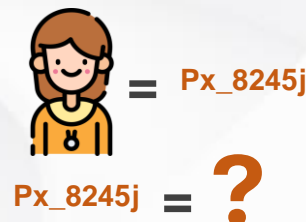
Seudonimización

Los datos se almacenan **sin estar directamente asociados** al interesado, pero pueden ser reidentificables.

Principales conceptos – Datos de carácter personal

Datos anonimizados

Aquellos sometidos a un proceso de anonimización, que implica que ya **no pueden asociarse** a una persona identificada o identificable, ni de manera directa ni indirecta, incluso mediante el uso de información adicional.

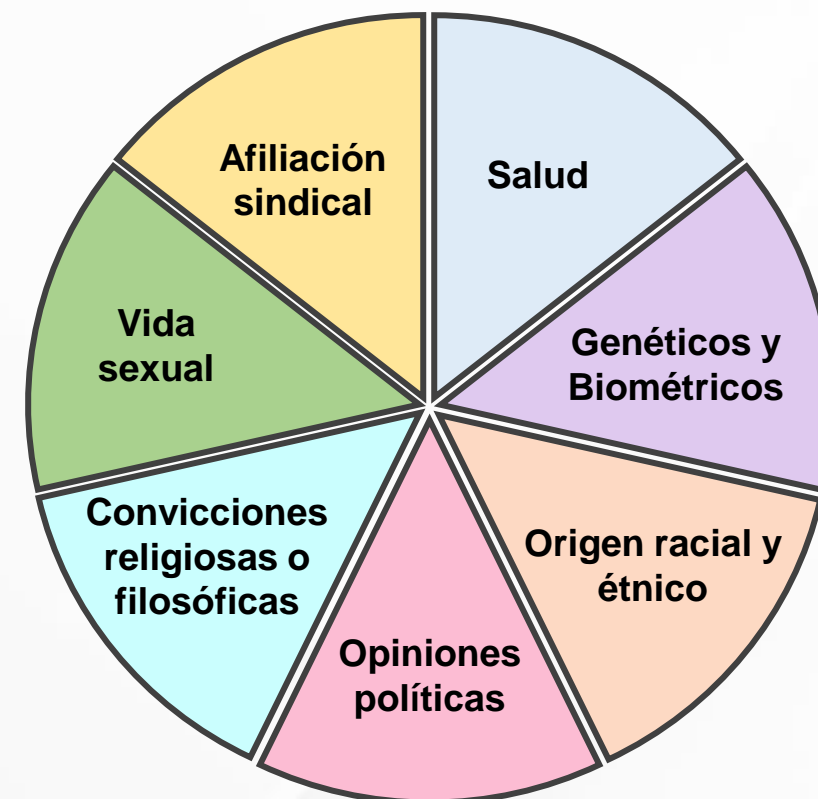


Categorías especiales de datos

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

En Europa se definen hasta 51 datos sensibles.

En el artículo 9 del RGPD se definen las **“Categorías especiales de datos”**.










Figuras principales

en el RGPD

Roles y responsabilidades

 Responsable del tratamiento	Persona física o jurídica, autoridad pública, servicio u otro organismo	Que determina los fines y medios del tratamiento.
 Encargado del tratamiento		Que trata datos por cuenta del responsable del tratamiento.
 Corresponsables del tratamiento		Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento.
 Destinatario		al que se comuniquen datos personales, se trate o no de un tercero.
 Interesado	Persona física	Sometida al tratamiento de sus datos personales.

Roles y responsabilidades

DPD

Persona experta encargada de **supervisar y garantizar** el cumplimiento de las normativas de **protección de datos** dentro de una organización. Sus funciones son:



1



Informar y asesorar sobre el tratamiento de datos personales.

2



Supervisar el cumplimiento del RGPD y LOPDGDD.

3



Aconsejar durante la evaluación de impacto.

4



Cooperar con las autoridades de control y actuar como punto de contacto.

5



Gestionar el tratamiento de datos teniendo en cuenta el riesgo.

6



Operar al más alto nivel jerárquico de la organización.

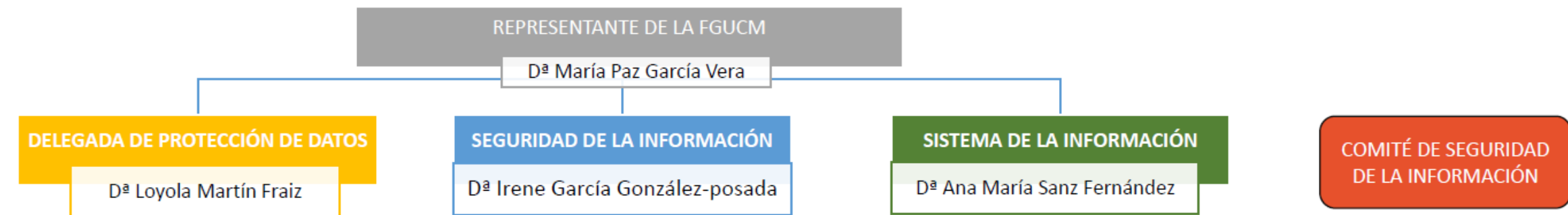
7



Asegurar el mantenimiento de la confidencialidad.



ROLES



RESPONSABLES DE SERVICIO/INFORMACIÓN

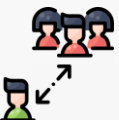




El nombramiento de un DPD es **obligatorio** en algunos supuestos, entre ellos: Fundaciones del sector público.



La figura de DPD será designada por sus **cualidades profesionales** en materia de protección de datos y su capacidad para desempeñar las funciones indicadas en el art. 39 del RGPD.



Tendrá una **posición independiente**, no podrá recibir instrucciones, ser sancionado ni destituido por otra persona de la organización.



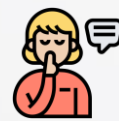
Tendrá una posición de más **alto nivel jerárquico**.



Tendrá **acceso a los recursos** necesarios para el ejercicio de sus funciones.



Se debe garantizar su **participación** en las cuestiones relativas a protección de datos personales.



Queda obligado a mantener el **secreto o confidencialidad**.



Delegado de protección de datos

Artículo 37 - 39

El DPD es la figura que actúa como contacto con la AEPD, además de asesorar a los responsables y encargados sobre las actividades de tratamiento.

Responsable del tratamiento

Artículo 37 - 39

Decide sobre la finalidad del tratamiento. Garantiza que el tratamiento es conforme a la normativa vigente.

Nombramientos

Nombramiento DPD comunicado a la AEPD: <https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf>
Información sobre Responsable de Tratamiento en web de FGUCM: <https://www.ucm.es/dpd>

Usuarios finales

Cooperar con el DPD proporcionando la información que necesite y pedirle asesoramiento sobre el tratamiento de los datos cuando se tengan dudas.

Encargados de tratamiento

Tratar los datos conforme a las instrucciones que reciban del Responsable del Tratamiento (FGUCM)

Implicaciones ENS



- Organización e implantación del proceso de seguridad, roles ENS:
 - Responsable de Información.
 - Responsable del servicio.
 - Responsable de seguridad.
 - Responsable del sistema.
 - Delegado de protección de datos (aplicabilidad RGPD/LOPDGDD).
- Incompatibilidades:
 - El responsable de Seguridad y el DPD no pueden ser la misma persona.
 - El responsable de Seguridad y el del sistema no pueden ser la misma persona, no puede existir dependencia jerárquica entre ellos.

ENS: artículo 13,

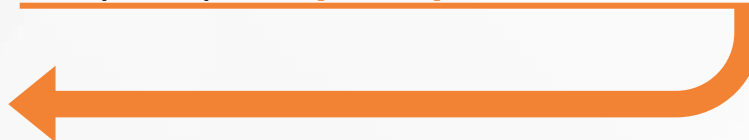


Principios rectores

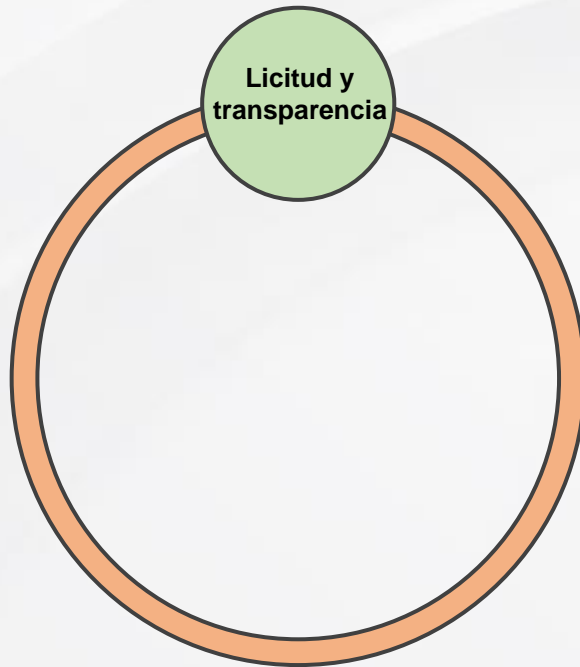


- Son los fundamentos sobre los cuales se basa todo el **tratamiento de datos personales**.
- Estos principios aseguran que los datos sean manejados de **manera justa, legal y segura**.

Los principales **principios rectores** del RGPD son:



Principios rectores – Licitud y transparencia



El interesado debe prestar su **consentimiento**.



El tratamiento es 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, siempre que no prevalezca sobre los derechos y libertades fundamentales del interesado

Consentimiento de los interesados



Artículo 7. Condiciones para el consentimiento

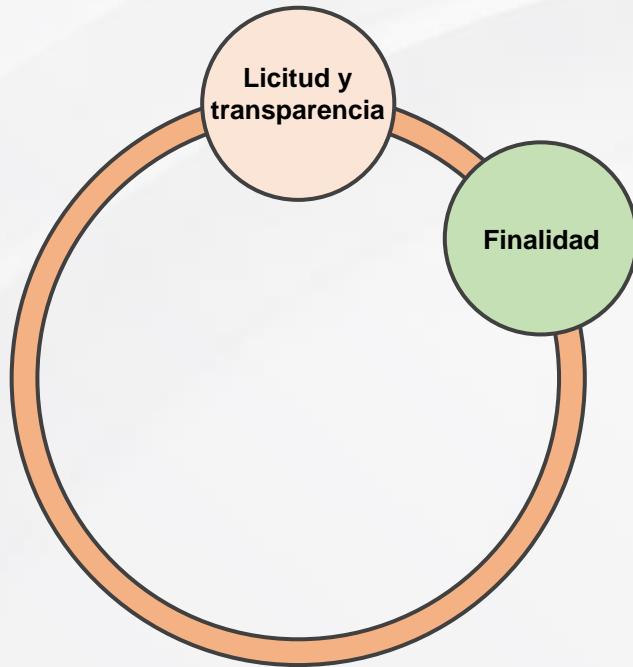
- El responsable debe poder **demostrar el consentimiento** del interesado.
- Si el consentimiento se da por escrito y se tratan más asuntos, el consentimiento a uno de ellos **no será vinculante** al resto.
- El interesado tendrá derecho a **retirar su consentimiento** en cualquier momento.
- El consentimiento no debe ser una **condición obligatoria para algo que no lo necesita**.



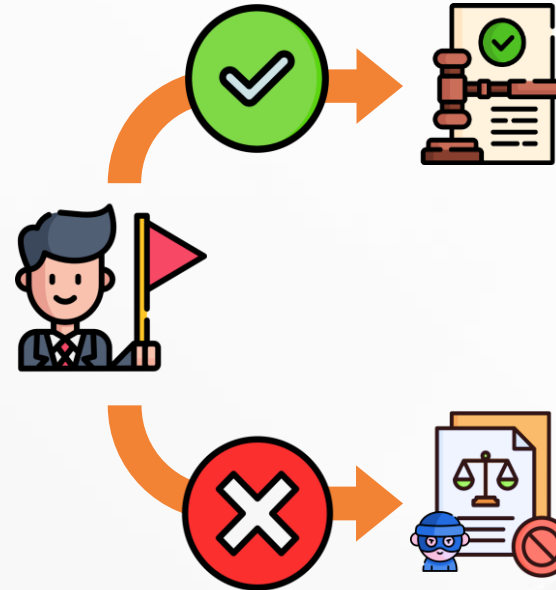
Artículo 9. Tratamiento de categorías especiales de datos personales

Incluso con consentimiento expreso del propietario de los datos, **NO** se podrán tratar los datos calificados dentro de la categoría de datos especiales.

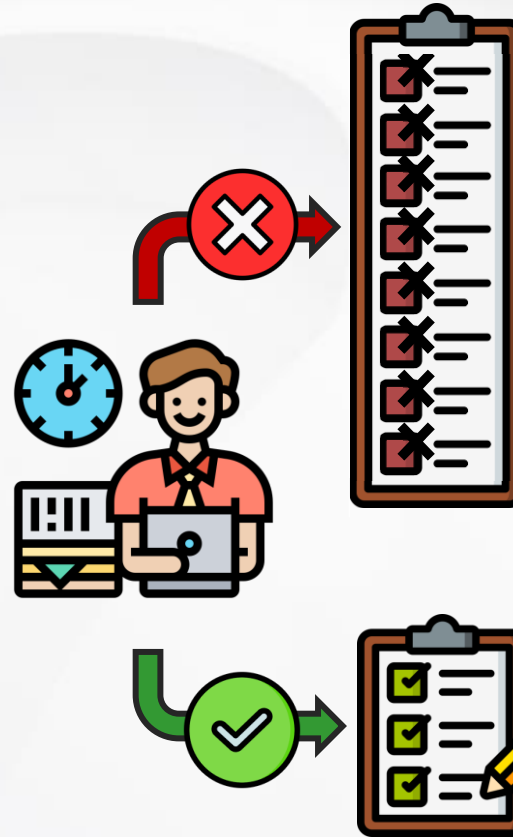
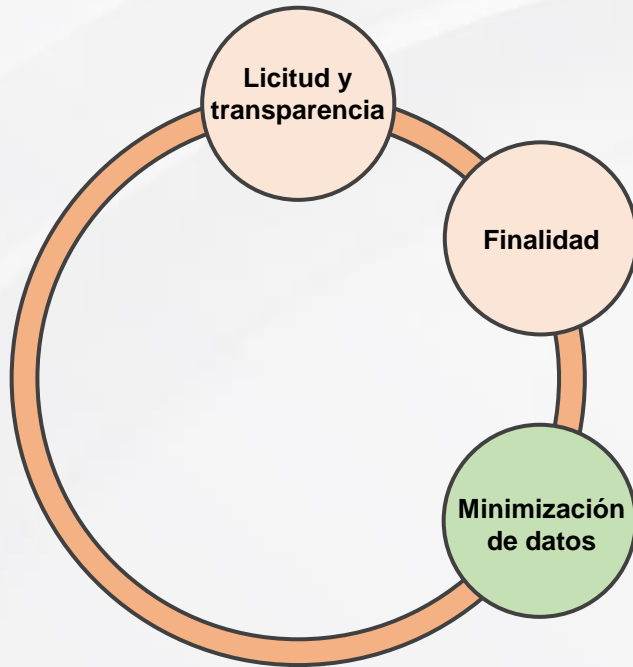
Principios rectores – Finalidad



Los datos personales deben ser recogidos con **fines específicos, explícitos y legítimos**, y no deben ser tratados de manera incompatible con esos fines.

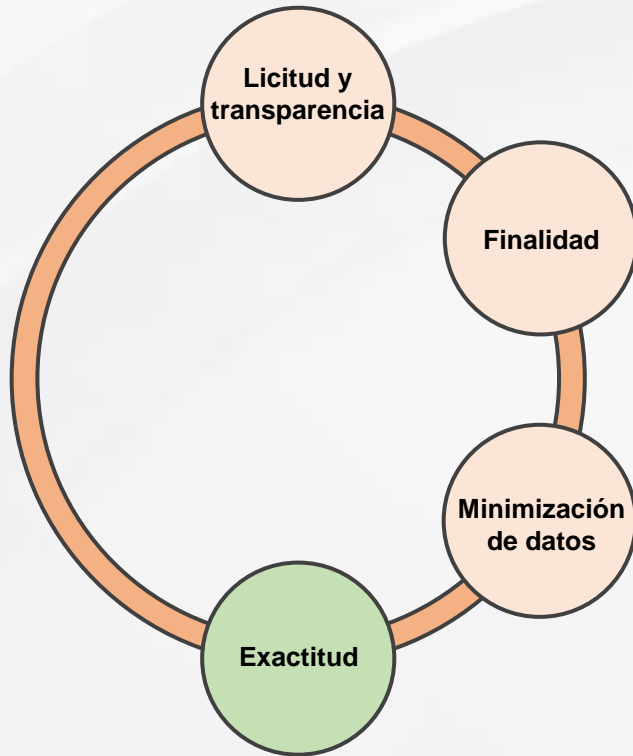


Principios rectores – Minimización de datos

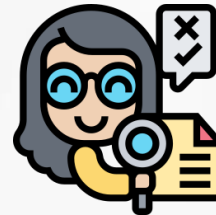


No es posible recabar y tratar datos simplemente “por tenerlos”

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

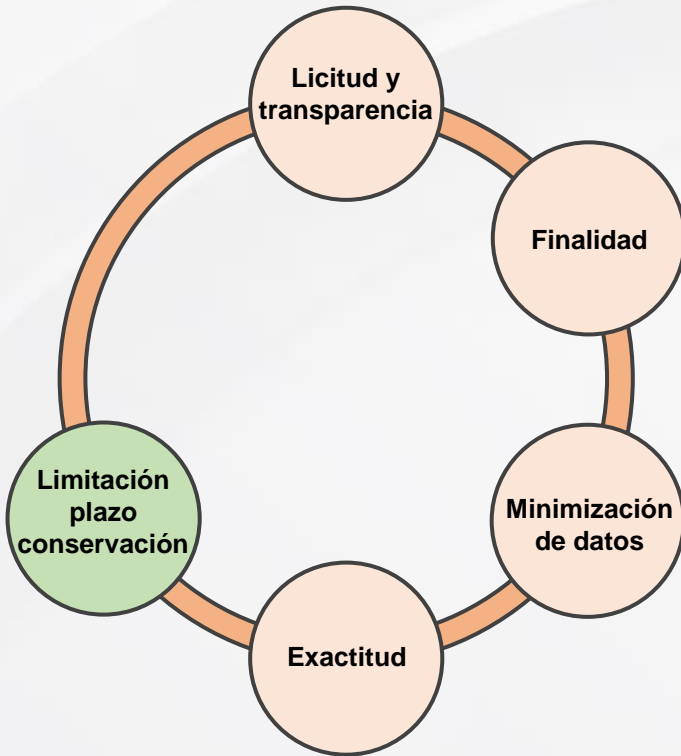


Los datos personales deben ser **exactos y estar actualizados**.

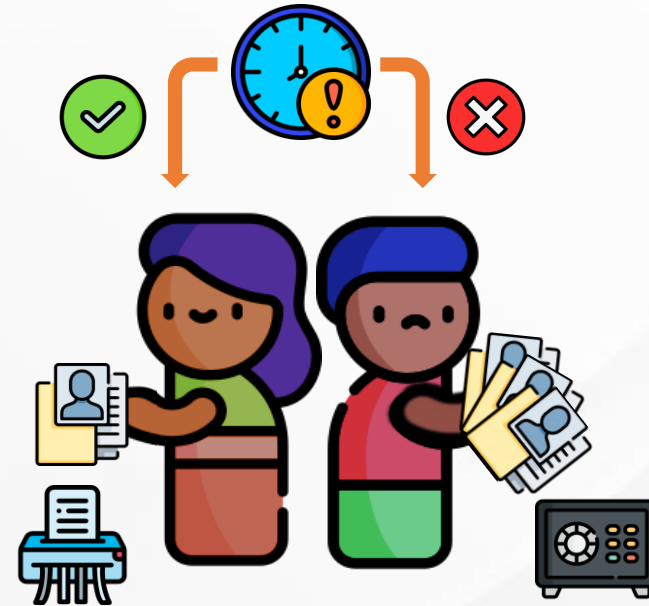


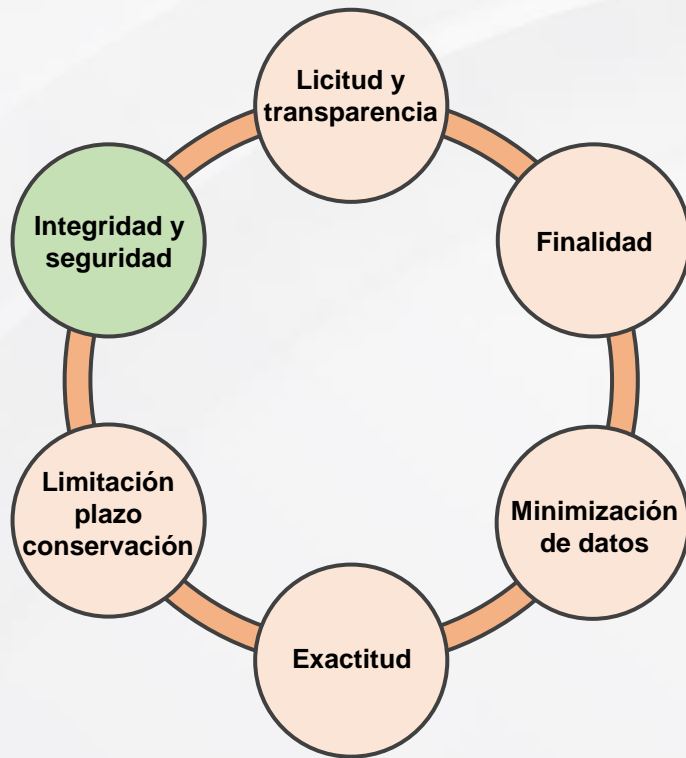
Se deben tomar medidas razonables para corregir o **eliminar los datos inexactos sin demora**.

Principios rectores – Limitación plazo conservación



- Los datos **no podrán ser mantenidos por más tiempo del necesario** para los fines del tratamiento.
- Superado este tiempo, tan solo podría conservarse con las finalidades de archivo de interés público, fines de investigación científica o histórica o fines estadísticos.





Los datos personales deben ser tratados de manera que se **garantice una seguridad adecuada**, mediante el uso de medidas técnicas y organizativas apropiadas.

Se debe asegurar la seguridad frente a:

- Tratamiento no autorizado o ilícito.
- Pérdida, destrucción o daño accidental.
- Cualquier otra vulneración a la confidencialidad.



Principios rectores – Responsabilidad proactiva

El **responsable del tratamiento** debe ser capaz de **demostrar** que cumple con los principios del RGPD. Esto incluye mantener registros de las actividades de tratamiento, realizar evaluaciones de impacto, y adoptar medidas de protección adecuadas.





Responsabilidad proactiva

Artículo 5

Se ha no solo de estar en disposición de dar cumplimiento a la normativa vigente sino demostrarlo activamente

Cultura de protección de datos

Se debe concienciar a todo el personal de FGUCM de la importancia del cumplimiento del RGPD y la LOPDGDD y la importancia de un correcto tratamiento de los datos personales que se manejan en el día a día. FGUCM tiene definido un documento general de Normativa de Protección de Datos que se ha de conocer.

Usuarios finales

Realizar el tratamiento de los datos si y solo si:

- Se tratan los datos necesarios con respecto a la finalidad y se tiene legitimidad para ello.
- Hay una ley que ampara el tratamiento de datos sin consentimiento y el proceso es legítimo.
- Se tratan con las debidas garantías.



Implicaciones ENS



- **Objeto del ENS:** asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios.
- **Principios básicos del ENS:**
 - Seguridad como proceso integral.
 - Gestión de la seguridad basada en los riesgos.
 - Prevención, detección, respuesta y conservación.
 - Existencia de líneas de defensa.
 - Vigilancia continua.
 - Reevaluación periódica.
 - Diferenciación de responsabilidades.
- **mp.si.5.** Eliminar de manera permanente y segura todo dato personal cuando sea requerido.

ENS: artículo 1 y 5



Obligaciones

de responsables y encargados del tratamiento

Obligaciones de responsables y encargados del tratamiento



Obligaciones de responsables y encargados del tratamiento

Requisitos del
contrato de encargo
de tratamiento



Establecerá objeto, duración, tipo de datos y categoría de interesados



El encargado tratará los datos siguiendo las instrucciones del responsable



Cualquier persona que trate los datos guardará confidencialidad



Medidas de seguridad a contemplar, incluyendo medidas ENS (op.ext)



Asistirá al responsable del tratamiento en la respuesta a ejercicio de derechos SOPLAR



El encargado pondrá a disposición del responsable toda la información necesaria que permita verificar cumplimiento de medidas de seguridad



A la finalización del contrato se destruirán o devolverán los datos objeto del encargo

Obligaciones de responsables y encargados del tratamiento



Obligaciones de responsables y encargados del tratamiento

Seguridad en la relación con proveedores

El responsable del tratamiento debe:



SEGUIMIENTO

Verificación y posibilidad de auditoría del cumplimiento de las obligaciones exigido por contrato



REGISTRO Y GESTIÓN DE CONTRATOS

Permite conocer la situación contractual de los proveedores



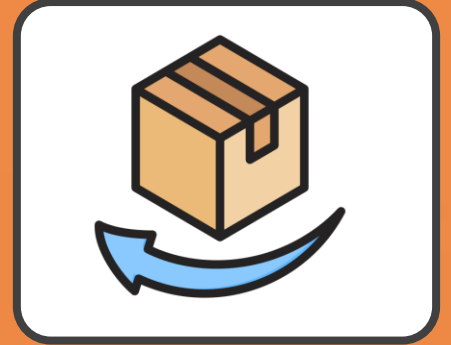
CUSTODIA

Y archivo de los contratos



MONITORIZACIÓN DE SLA'S

Convendrá tener en consideración los tiempos de respuesta y las 72 horas de comunicación de las brechas de seguridad



DEVOLUCIÓN DE ACTIVOS Y SOPORTES

Devolución y destrucción de la información

Obligaciones de responsables y encargados del tratamiento

Encargado de tratamiento versus Proveedor



Encargado de tratamiento versus Proveedor

Artículo 28

El encargado del tratamiento tratará los datos conforme a las instrucciones recibidas por parte del responsable del tratamiento.

Procedimiento

Antes de contratar a un encargado del tratamiento, se verificará que está en condiciones de prestar el servicio garantizando la seguridad de la información de FGUCM y se deberá firmar clausulado de encargo de tratamiento que incluya exigencias ENS, siguiendo las indicaciones de la normativa de protección de datos establecida por FGUCM

Usuarios finales

Los empleados del encargado del tratamiento y toda la cadena de suministro respetarán el deber de confidencialidad, y las directrices del responsable del tratamiento para la ejecución del encargo



Implicaciones ENS



Recursos externos:

- **op.ext.1:** ANS con las características del servicio, el «servicio mínimo admisible», la responsabilidad del prestador y las consecuencias de incumplimientos.
- **op.ext.2:** sistema rutinario para medir el cumplimiento de las obligaciones del servicio.
- **op.ext.3:** protección de la cadena de suministro (AR, continuidad, gestión de la seguridad).
- **op.ext.4:** interconexión de sistemas para el intercambio de información-

ENS: op.ext 1, op.ext 2, op.ext 3 y op.ext 4

Deber de información

Al **recoger datos personales** de un interesado, se le debe **facilitar** la siguiente información:



Identidad y datos de contacto

del responsable y del DPD



Los fines del tratamiento

a que se destinan los datos personales y la base jurídica del tratamiento.



Licitud

Del consentimiento y el tratamiento



La intención de

transferencia internacional de los datos personales, si la hubiese.



Destinatarios

o las categorías de destinatarios de los datos.



Plazo de conservación

de los datos.



La existencia de los **derechos de los interesados.**



Derecho a presentar una reclamación ante la autoridad de control

Además...

Cuando se quieran utilizar los datos personales para un **fin distinto** al aceptado por el interesado, se le debe informar y solicitar su consentimiento.



Deber de Información

Artículos 13-14

Se debe informar a los interesados de la finalidad del tratamiento de sus datos, además de otras informaciones de relevancia.



Procedimientos de protección de datos

FGUCM cuenta con una normativa de protección de datos y con cláusulas informativas a los afectados, no obstante, estas cláusulas han de revisarse periódicamente y mantenerse actualizadas.



Usuarios finales

Cuando se vayan a tratar datos personales, adjuntar en el proceso de recogida todas las cláusulas necesarias para el cumplimiento de RGPD y LOPD.

Implicaciones ENS



- **op.pl.1:** una correcta gestión de riesgos asegura que las amenazas a los datos personales se minimicen, lo que, a su vez, permite a las organizaciones comunicar con precisión a los interesados cómo se protege su información.

ENS: op.pl.1

Área económica-financiera

DATOS PERSONALES Y FISCALES	
GRUPO I	APELLIDOS: <input type="text"/> NOMBRE: <input type="text"/> Nº NIF: <input type="text"/> Nº PASAPORTE: <input type="text"/> DIRECCIÓN: <input type="text"/> POBLACIÓN: <input type="text"/> PROVINCIA: <input type="text"/> C.P.: <input type="text"/> EMAIL: <input type="text"/> TELÉFONO/S: <input type="text"/>

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS:	
RESPONSABLE DEL FICHERO:	Fundación General de la Universidad Complutense de Madrid
FINALIDADES:	Gestionar el pago como Proveedor y cliente de nuestras actividades. Enviarle información de su interés.
LEGITIMACIÓN:	Contrato del que usted forma parte y Consentimiento.
DESTINATARIOS:	No se cederán sus datos de carácter personal, salvo obligación legal.
DERECHOS:	Acceder, rectificar y suprimir los datos así como otros derechos que puede consultar en la Información adicional.
INFORMACIÓN ADICIONAL:	Puede consultar toda la información adicional en: https://www.ucm.es/fundacion/file/informacion-adicional-colaboradores.proveedores

Fundación General de la Universidad Complutense de Madrid. Área Económica - Financiera

Declaro al marcar esta casilla que: no viene desempeñando puesto o actividad en el Sector Público delimitado en el art.1 de la Ley 53/5984 de Incompatibilidades, entendiéndose dentro del Sector Público todas las Administraciones Públicas, incluida la Administración de Justicia y los Entes, Organismos y Empresas en ella dependientes, incluso las entidades colaboradoras y concertadas de la Seguridad Social en la gestión sanitaria. Ni superar los 18.000 euros anuales.

DATOS BANCARIOS
NOMBRE DE LA ENTIDAD BANCARIA:
I.B.A.N. (International Bank Account Number). RELLENAR LOS 24 DÍGITOS:

Madrid, de de 20

Firma:

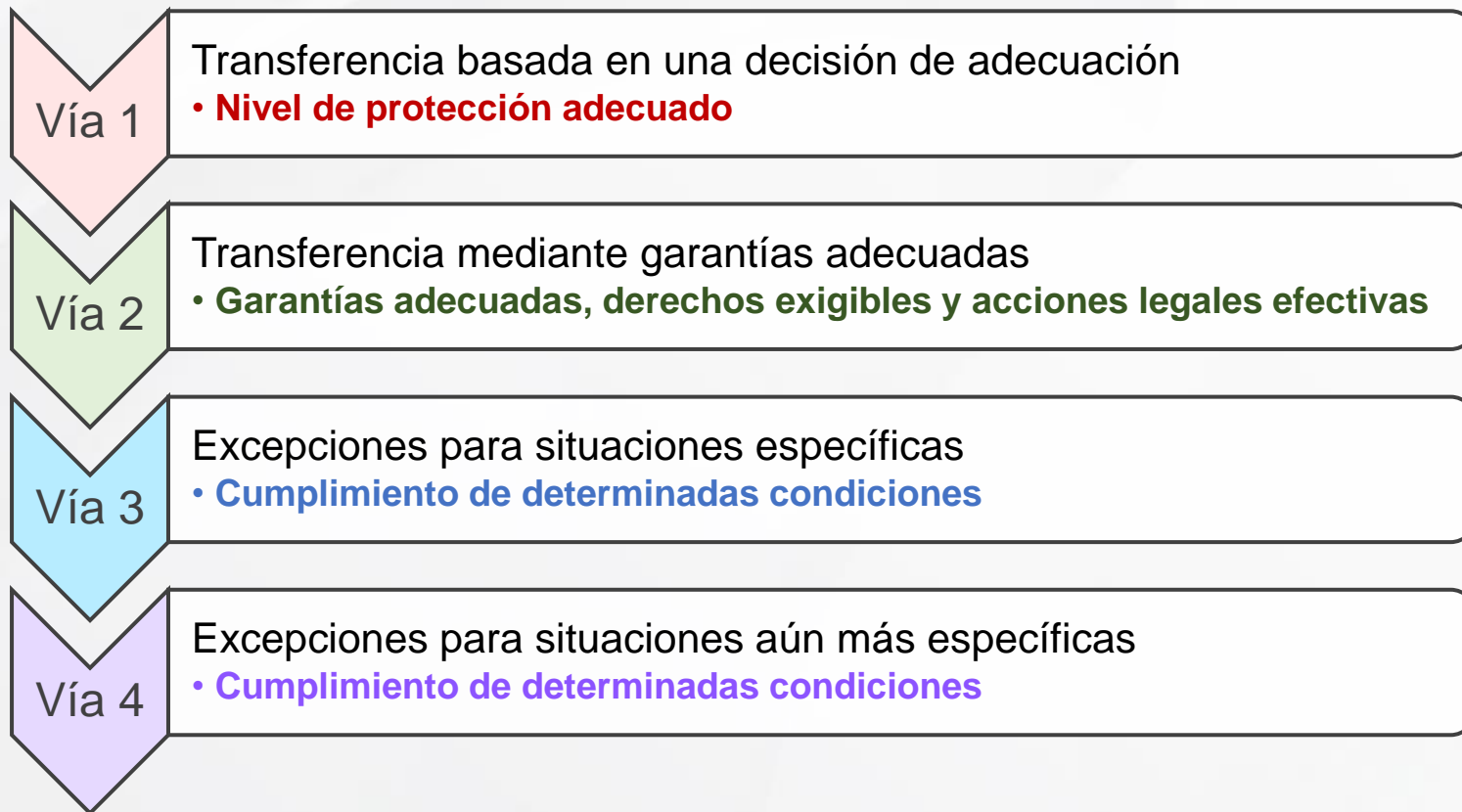
Imprimir

Le informamos de la base legal sobre la que se desarrolla el tratamiento de sus datos con fines de gestionar el pago como Proveedor y cliente de nuestras actividades, dicho tratamiento se encuentra amparado dentro de las bases legitimadoras del tratamiento que establece el Reglamento Europeo de Protección de datos 2016/679, ya que es necesario para gestionar un contrato o precontrato en el que usted es parte. Además de contar con su consentimiento, queremos informarle de:

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS:	
RESPONSABLE DEL FICHERO:	Fundación General de la Universidad Complutense de Madrid
FINALIDADES:	Gestionar el pago como Proveedor y cliente de nuestras actividades. Enviarle información de su interés.
LEGITIMACIÓN:	Contrato del que usted forma parte y Consentimiento.
DESTINATARIOS:	No se cederán sus datos de carácter personal, salvo obligación legal.
DERECHOS:	Acceder, rectificar y suprimir los datos así como otros derechos que puede consultar en la Información adicional.
INFORMACIÓN ADICIONAL:	Puede consultar toda la información adicional en: https://www.ucm.es/fundacion/file/informacion-adicional-colaboradores.proveedores

Transferencias Internacionales

Suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).



Países fuera de la UE
a los que se **permite** la transferencia:

Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Japón, Reino Unido, Corea del Sur, USA (Data Privacy Framework)

Transferencias Internacionales



Transferencias Internacionales

Artículo 44 - 46

La transferencia de datos a otros países de la UE se podrá realizar si hay consentimiento expreso del interesado, la transferencia es afín a la finalidad del tratamiento y existen garantías de seguridad.

Procedimiento de Transferencias Internacionales de Datos

Desde FGUCM no se realizan Transferencias Internacionales de Datos, pero si así fuera, se debe realizar un procedimiento específico para su correcta gestión.

Usuarios finales

No realizar ninguna transferencia internacional si no tiene autorización del responsable.



Implicaciones ENS



- **mp.cpm.1:** sistema de protección perimetral que separe la red interna del exterior.
- **mp.cpm.2:** redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.
- **mp.cpm.3:** comunicaciones con puntos exteriores, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información.
- **mp.cpm.4:** separación de flujos de información en la red.

ENS: mp.com, protección de las comunicaciones



Registro de las actividades del tratamiento (RAT)



- 1 Facilita transparencia
- 2 Sirve como herramienta para el control de las autoridades de supervisión
- 3 Ayuda a las organizaciones a documentar y controlar sus tratamientos
- 4 Debe estar publicado en el caso de FGUCM al ser AAPP
- 5 Debe estar permanentemente actualizado

Registro de Actividad de Tratamiento

Obligatorio para responsables y encargados del tratamiento.



Responsable del tratamiento

- Nombre y datos de contacto del responsable, representante del responsable y DPD.
- Los fines del tratamiento.
- Descripción de las categorías de interesados y de datos tratados.
- Categorías de destinatarios, incluidas transferencias internacionales.
- Plazos previstos para la supresión de los datos.
- Descripción general de las medidas técnicas y organizativas de seguridad.



Encargado del tratamiento

- Nombre y los datos de contacto del encargado, de cada responsable por cuenta del cual actúe y del DPD.
- Categorías de tratamientos realizados por cuenta de cada responsable.
- Transferencias internacionales de datos.
- Descripción general de las medidas técnicas y organizativas de seguridad que se aplican.

Ejemplos de tipologías de tratamientos



	Recogida
	Registro
	Estructuración
	Conservación
	Modificación

	Extracción
	Consulta
	Comunicación
	Difusión
	Cotejo

	Interconexión
	Destrucción
	Elaboración de perfiles
	Decisiones automatizadas
	Transferencias Internacionales



Registro de Actividad de Tratamiento

Artículo 30

Se debe mantener un registro de actividades de tratamiento que indique toda la información necesaria para que los encargados puedan tratar los datos de la manera más adecuada.

Procedimientos de Registros de actividad

FGUCM tiene publicado su RAT en la web corporativa:

<https://www.ucm.es/fundacion//registro-de-actividades-de-tratamiento>

Usuarios finales

El RAT debe mantenerse actualizado, los usuarios están obligados a comunicar al RT y al DPD cualquier cambio en los mismos, así como el inicio de un nuevo tratamiento para su correspondiente análisis de riesgos y EIPD si procede.



Implicaciones ENS



- **op.pl.1:** análisis de riesgos (AR) partiendo de los activos más importantes, la actividad de tratamiento (información) puede ser el punto de partida para la realización del AR.
- **op.exp.1:** al igual que el ENS requiere que se mantenga un inventario de activos, los tratamientos de datos han de mantenerse inventariados y actualizados, en relación con los activos que define el ENS y que tienen relación con los tratamientos de datos (p.ej.: sistemas de información).
- **mp.info.1:** el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el RT con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de información.

ENS: op.pl.1, op.exp.1 y mp.info.1

Registro de Actividades de Tratamiento

Actividades de Tratamiento

- Colaboradores / Proveedores
- Comité de empresa
- Formación
- Patronos
- Promociones inmobiliarias
- Recursos humanos
- Congresos
- Formación continua
- Investigación
- Prácticas en empresas

La publicación de este inventario se realiza en cumplimiento del artículo 30 del Reglamento (UE) 2016/679 (RGPD) y del Art. 31 de la Ley Orgánica 3/2018 (LOPDGDD).

ACTIVIDAD DE TRATAMIENTO - RRHH	
Responsable de tratamiento	Fundación General de la UCM N.I.F./C.I.F. G-79485082 Dirección postal: Calle Doctor Severo Ochoa nº 7, 28040-Madrid Teléfono: 913946362/913946493 Correo electrónico: protecciondedatos@rect.ucm.es Delegado de protección de datos: dpofgu@ucm.es
Fines del tratamiento	Gestionar la relación laboral y todas las gestiones que de ésta se deriven, así como las nóminas del personal de la FGUCM.Expediente personal.Control horario.Formación.Acción social.prevencción de riesgos laborales.Gestión económica de la acción social.
Base jurídica	RDPD: 6.1b) Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. RGPD: 6.1C) Tratamiento necesario par el cumplimiento de una obligación legal aplicable al responsable del tratamiento Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. Ley General Tributaria
Tipología de la finalidad	Empleados.
Colectivo	Empleados y sus familiares.
Categorías de datos	Identificativos:Nombre y apellidos, DNI/CIF, número de resgistro de personal,número de Seguridad Social/dirección, firma y teléfono.Datos de características personales:Sexo, estado civil, nacionalidad, edad, fecha y lugar de nacimiento y datos familiares.Datos de circunstancias familiares;fecha de alta y baja,licencias, permisos y autorizaciones.De acuerdo al principio de minimización de datos. Personales:datos de salud(bajas por enfermedad, accidente laborales y grado de discapacidad,sin inclusión de diagnóstico), afiliación sindical, a los exclusivos efectos del pago de cuotas sindicales(en su caso),representación sindical (en su caso), justificantes de asistencia de propios y de terceros. Económico-financieros: nómina, créditos, préstamos, avales,retenciones judiciales(en su caso), otras retenciones(en su caso) Datos bancarios. Académicos y profesionales:Titulaciones, Formación y experiencia profesional.Datos de detalle de empleo.Datos de control de presencia;fecha/hora entrada y salida, motivo de ausencia. Otros datos:datos relativos a la acción social, datos sobre sanciones en materia laboral. Categoría especial de datos: afiliacion sindical, salud.
Categorías de destinatarios	Tesorería general de la Seguridad Social,Instituto Nacional de la Seguridad Social, Mutua de accidente de trabajo y enfermedad profesional y Sociedad de Prevención de riesgos laborales, Tribunal de Cuentas de la Comunidad de Madrid, Cámara de Cuentas de la Comunidad de Madrid,Entidades financieras. Agencia Estatal de la Administración Tributaria
Periodo de conservación/Plazos conservación	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para detreminar las posibles responsabilidades derivadas del tratamiento. Posteriormente, la conservación o, en su caso, la supresión se realiza conforme a la normativa vigente.
Medidas técnicas y organizativas de seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Documento de Seguridad (Anexo II y siguientes), y del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, documentos que conforman la Política de protección de datos y seguridad de la Información de la FGUCM.
Transferencia Internacional de datos	No están previstas transferencias internacionales de los datos



Derechos de los afectados

Derechos de los afectados

Los interesados del tratamiento tienen los siguientes **derechos**:

Acceso



A conocer, de forma concisa y transparente:

- Si sus datos están siendo tratados.
- Finalidad del tratamiento.
- Quienes son los destinatarios.

Además, derecho a recibir copia de sus datos.

Supresión



- A que sus datos sean eliminados.
- A retirar el consentimiento en cualquier momento.

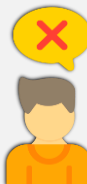
Portabilidad de los datos



A transmitir datos directamente a otro responsable del tratamiento sin que nadie lo impida.



A conocer la **obligación** de dar los datos para el tratamiento (ej. contrato) y las consecuencias de no darlos.



Oposición

A oponerse en cualquier momento al tratamiento de sus datos.



Rectificación

A obtener la rectificación de los datos personales inexactos.



Limitación del tratamiento

A que sus datos no se utilicen para nada más que lo estrictamente aceptado.



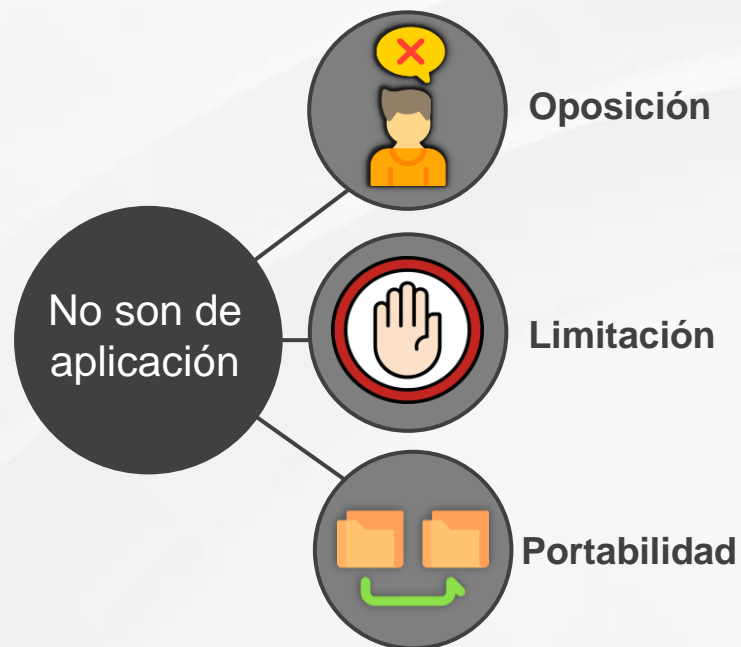
A presentar una **reclamación** ante una autoridad de control.



A conocer la existencia de **decisiones automatizadas** y la fuente de la que proceden.

Derechos de los afectados

Algunos de los **derechos** no son de aplicación o son de aplicación limitada en la administración pública debido a que:



Porque el tratamiento es **necesario para garantizar**

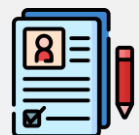
- La seguridad y la salud de las personas
- La libertad de expresión e información
- El cumplimiento de obligaciones legales
- Razones de interés público, como salud pública
- Fines de investigación o estadísticos
- Formalizar el ejercicio o defensa de reclamaciones

En cualquiera de los casos ...



El responsable del tratamiento está **obligado a responder en todo caso** a las solicitudes del interesado de forma motivada a más tardar en el plazo de **un mes**, sea aceptada o no.

Dicho plazo podrá **prorrogarse otros dos meses** en caso necesario (3 meses en total), teniendo en cuenta la complejidad y el número de solicitudes (artículo 12 RGPD), se debe informar de dicha prórroga dentro del plazo del primer mes de forma motivada.



Además, se llevará un **registro** de:

- Las actividades de tratamiento efectuadas
- Los derechos solicitados por los interesados.



Derechos de los interesados

Artículo 15 -22

Son una serie de derechos que se otorgan a las personas sobre el tratamiento de sus datos personales. Estos derechos son fundamentales para garantizar la transparencia, control y protección de los datos personales en la era digital.



Procedimiento de los derechos de personas interesadas

FGUCM dispone de un procedimiento para gestionar los derechos de los interesados y los modelos de formularios para tramitar los mismos. **MARCO JURÍDICO. DERECHOS**

Usuarios finales



1. Usar los formularios establecidos.
2. Solicitar la documentación al interesado.
3. Tramitar la solicitud en los plazos establecidos.
4. Llevar a cabo las acciones según tipo de solicitud.
5. Contestar al interesado.

Implicaciones ENS



- **Acceso:** evitar el acceso no autorizado para ello se ha de asignar permisos adecuados a la información y realizar revisiones periódicas (op.acc)
- **Custodia:** almacenar la información de forma segura (mp.si.3).
- **Incidentes:** reportar incidente de seguridad (op.exp.7)
- **mp.info.5:** Se tomarán precauciones frente a la información oculta que pueda revelar datos confidenciales, especialmente si son de carácter personal, como los metadatos

ENS: op.acc, op.exp.7, op.exp.9, mp.si.3, mp.info.1



Proveedores

Obligaciones de responsables y encargados del tratamiento

¿Puede contratarse cualquier proveedor?



Encargado del tratamiento

Disposición Adicional 25ª

LCSP

RGPD

Considerando 81

Artículo 28.3

RGPD

LOPDgdd

Disposición Adicional 1ª

Obligaciones de responsables y encargados del tratamiento

¿Puede contratarse cualquier proveedor?



Si la contratación implica el **acceso del contratista a datos personales** de cuyo tratamiento sea responsable la entidad contratante, **aquel tendrá la consideración de encargado del tratamiento**

(...) al encomendar actividades de tratamiento a un encargado, **debe recurrir únicamente a encargados que ofrezcan suficientes garantías**



El tratamiento por el encargado **se regirá por un contrato** u otro acto jurídico con arreglo al Derecho

Si un tercero preste un servicio de concesión, gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y **se ajustarán al Esquema Nacional de Seguridad**





Controles y Medidas de seguridad

en el tratamiento de datos personales

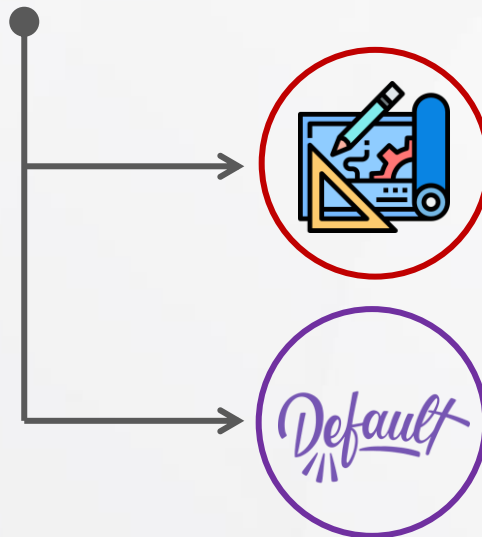
Protección de datos desde el diseño y por defecto



Principio fundamental del RGPD
Enfoque proactivo

La protección de datos debe estar integradas en:

- Procesos de desarrollo y operación
- Servicios que traten datos, desde el principio y por defecto



Privacidad desde el diseño

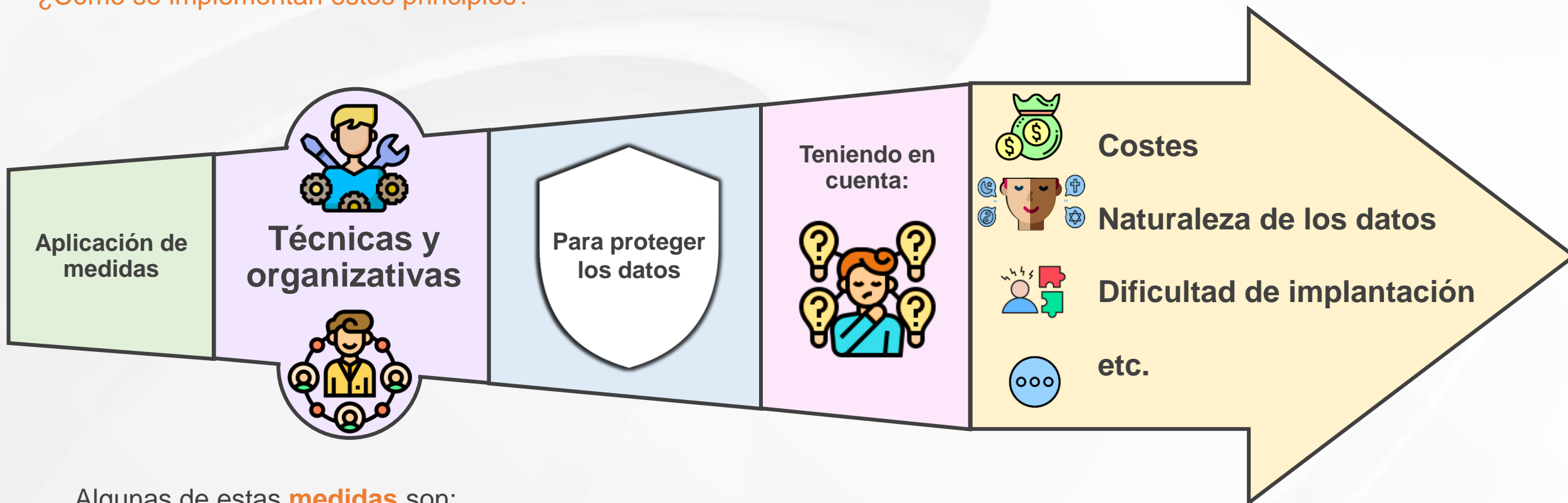
- Integración temprana
- Medidas técnicas y organizativas
- EIPD
- Durante todo el ciclo de vida del dato

Privacidad por defecto

- Minimización de datos
- Configuración predeterminada
- Control de acceso
- Facilidad para los usuarios

Protección de datos desde el diseño y por defecto

¿Cómo se implementan estos principios?



Algunas de estas **medidas** son:



Seudonimización



Criptografía



Protección con contraseña



Destrucción y borrado seguro

Protección de datos desde el diseño y por defecto



Protección de datos desde el diseño y por defecto

Artículo 25

Se debe asegurar que las actividades de tratamiento tienen las garantías necesarias para asegurar la seguridad de los datos.



Procedimientos de protección de datos

FGUCM cuenta con procedimientos generales de protección de datos, así como con un cuerpo normativo ENS para la adopción de estos principios fundamentales del RGPD.



Usuarios finales

Conocer y aplicar todas las medidas técnicas y organizativas a disposición para asegurar que las actividades de tratamiento son correctas y seguras.

Implicaciones ENS



- **El ENS** aplica en estos supuestos en toda su extensión.
- **El ENS** proporciona el marco de seguridad necesario para garantizar que las organizaciones puedan cumplir adoptar la seguridad desde el diseño y por defecto durante todo el ciclo de vida de los datos, asegurando que los datos personales sean tratados de manera segura y transparente.

ENS

Medidas de seguridad

Principales obligados

Disposición adicional primera LOPDGDD: Medidas de seguridad en el ámbito del sector público

El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

Entidades obligadas a cumplir:



Medidas de seguridad – Sistemas, aplicaciones o servicios comprendidos en el ENS

Sedes electrónicas

Registros electrónicos

Sistemas de información accesibles electrónicamente por los ciudadanos

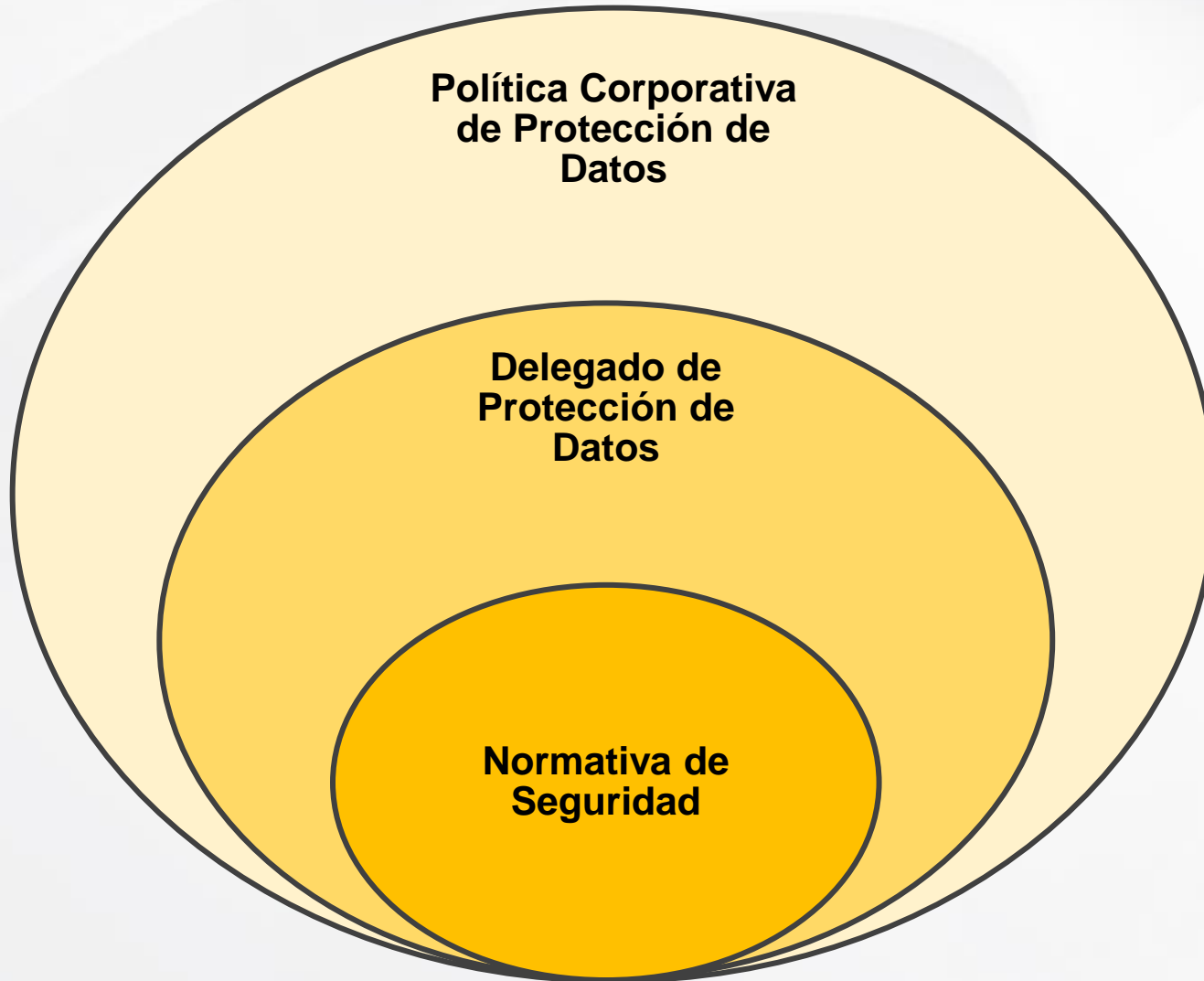


Sistemas de información para el ejercicio de derechos

Sistemas de Información para el cumplimiento de deberes.

Sistemas de Información para recabar información y estado del procedimiento administrativo

Medidas de seguridad – Estructura organizativa interna



Medidas de seguridad – Obligación de medios

Indica el Tribunal Supremo que será exigible a los responsables y encargados del tratamiento:

Adopción e implantación de medidas

Técnicas y Organizativas

Conformes al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión.

Deben evitar la alteración, pérdida, tratamiento o acceso no autorizado.



CONSEJO GENERAL DEL PODER JUDICIAL

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



Detección y reacción

frente a brechas de seguridad

Brechas de seguridad

Si un incidente **pone en peligro** los datos personales de los interesados, **se deberá comunicar**.

1

A las autoridades

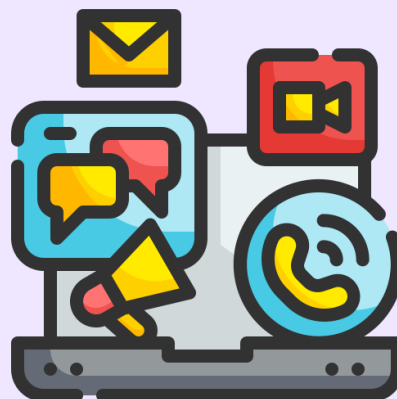
Sin dilación indebida, en un **plazo máximo de 72 horas**, siempre que el incidente ponga en peligro los datos personales.



2

A los interesados

De manera **individual** o **pública**, si es de alto riesgo para los derechos y libertades y/o repercute a muchos interesados.



*

No será necesario

Si los datos involucrados están **protegidos**.



Brechas de seguridad

La **notificación** de la brecha a la AEPD debe contener:



Naturaleza del incidente, incluyendo las categorías y el número aproximado de afectados.



Nombre y los datos de contacto del delegado de protección de datos.

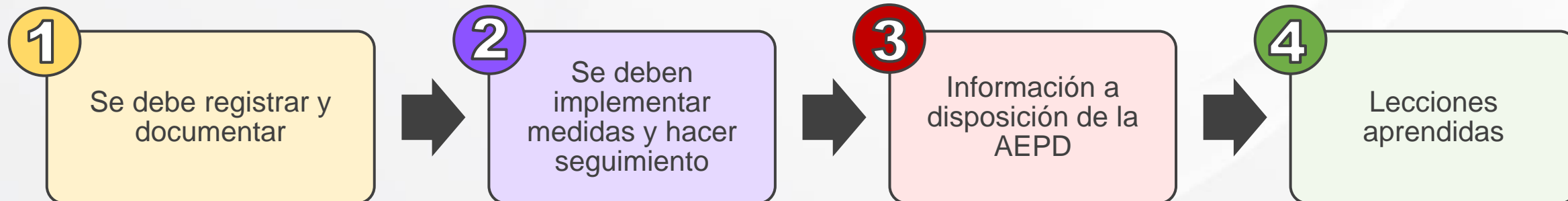


Posibles consecuencias de la violación de la seguridad de los datos personales.

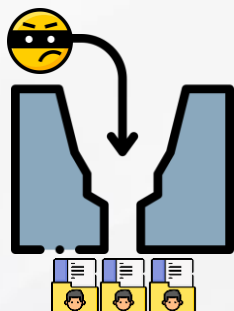


Medidas adoptadas por el responsable del tratamiento para poner remedio a la violación de la seguridad.

Además de comunicarlo, se deben seguir los siguientes pasos:



Brechas de seguridad

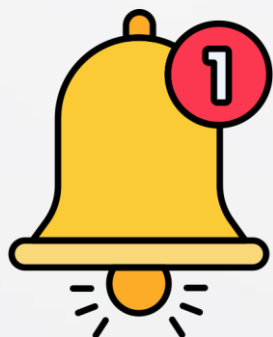
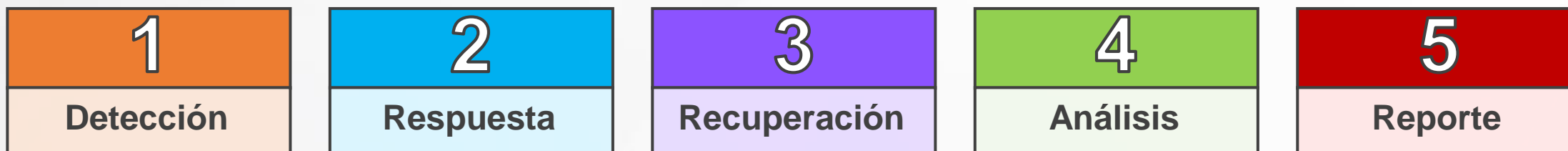


Incidentes de seguridad ENS

Pueden afectar a datos personales y ser a su vez una brecha de seguridad.

La correcta gestión de estos incidentes es crucial para garantizar que los daños sean minimizados y que se tomen medidas correctivas adecuadas.

La **gestión de incidentes de seguridad** según el ENS implica varios **pasos clave**:



Guía nacional de notificación y Gestión de ciberincidentes

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

Comunicación al CCN



incidentes@ccn-cert.cni.es

Si afecta a datos personales





Brechas de seguridad

Artículo 33 - 34

Ante un incidente de seguridad que afecte a los datos personales, se debe notificar cuanto antes a la AEPD, informando sobre el incidente y las medidas aplicadas para mitigarlo. Se deberá informar a los interesados si resulta necesario.

Procedimiento de gestión de riesgos

Se debe notificar y formar a todo el personal el procedimiento de notificación de violaciones de seguridad y de gestión de incidentes, para que puedan identificarlos fácilmente en su caso y conozcan el procedimiento de escalado para su gestión y notificación.

Usuarios finales

Notificar al responsable, cuanto antes, sobre la sospecha u ocurrencia de un incidente de seguridad, pueda o no afectar a los datos personales.



Implicaciones ENS



- **Gestión de incidentes (op.exp.1 y op.exp.2):**
 - Proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema.
 - Detección y respuesta: implantación de medidas, asignación de recursos, información a responsable de información y del servicio.
 - Prevención para evitar que los incidentes se repitan.
 - La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el RGPD.

ENS: op.exp.1, op.exp.2

Implicaciones ENS

Registro de la gestión de incidentes (op.exp.9)

- Se han de registrar todos los incidentes de seguridad (reportes iniciales, intermedios y finales de los incidentes).
- Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional.
- Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

ENS: op.exp.9



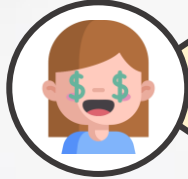
Evaluación de Impacto

Evaluación de Impacto

Cuando sea probable que un tipo de tratamiento entrañe un **alto riesgo**, se realizará una **evaluación del impacto**. Deberá incluir como mínimo:



Descripción de operaciones y **finés del tratamiento**.



Interés legítimo perseguido por el responsable.



Necesidad y proporcionalidad del tratamiento con respecto a su finalidad.



Riesgos para los derechos y libertades de los interesados.



Las **medidas y garantías** para afrontar los riesgos.

Evaluación de Impacto

Cuando la evaluación de impacto entrañe un **alto riesgo**, se realizará una **consulta previa**.



Consulta previa a la AEPD



Se informa a la AEPD de **finés de tratamiento y medidas implantadas**



Plazo de contestación 8 semanas asesorando al Responsable del tratamiento



Según complejidad el plazo de puede alargar otras 6 semanas, la AEPD informará de esto dentro del primer mes de la recepción de la solicitud



Evaluación de Impacto

Artículo 35 - 36

Se debe evaluar el impacto de un posible incidente de seguridad que pueda afectar a los datos personales antes de tratarlos. En caso de requerirlo, se puede solicitar asesoramiento a las autoridades de control.



Procedimiento evaluación de impacto

De forma previa a comenzar un tratamiento se hará EIPD, si tras aplicar medidas el riesgo sigue siendo alto, se hará consulta previa a la AEPD para su asesoramiento y respuesta sobre el tratamiento.



Usuarios finales

Cooperar con los responsables de realizar el análisis de impacto, proporcionando la información que resulte necesaria.

Implicaciones ENS



- Sistemas de información que traten datos personales.
- El Responsable o el encargado del tratamiento, asesorados por el DPD realizarán un análisis de riesgos de protección de datos y en su caso una EIPD.
- Prevalecerán las medidas a implantar del análisis de riesgos y de la EIPD en caso de resultar agravadas respecto de las previstas en el ENS.
- **op.pl.1:** análisis de riesgos
- **mp.cont.1:** se realizará análisis de impacto de las operaciones de tratamiento llevadas a cabo.

ENS: artículo 3, op.pl.1



Autoridades de control

Autoridades de referencia

Protección de datos



REGIONALES



Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos



Consejo de Transparencia y Protección de Datos de Andalucía



Ciberseguridad



Autoridades de referencia

AEPD



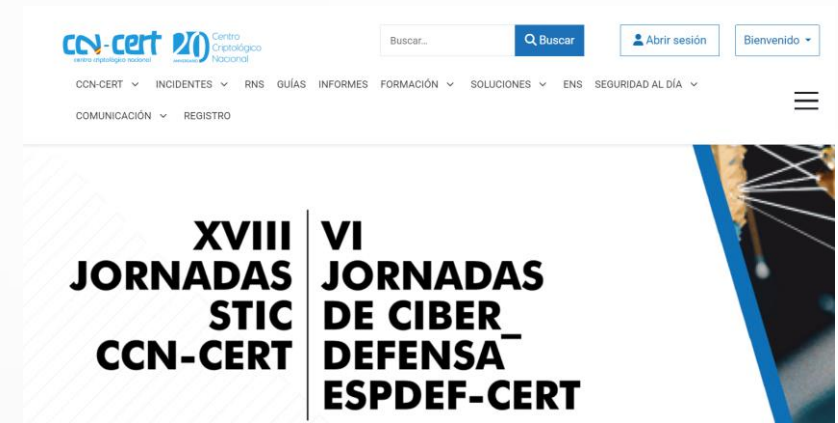
<https://www.aepd.es/>

EDPB



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

CCN-CERT



<https://www.ccn-cert.cni.es/es/>



Infracciones y sanciones

Infracciones sobre...

RGPD

GRAVES

- Obligaciones de:
- Responsables y encargados (*art. 8, 11, 25 a 29, 42 y 43*).
 - Organismos de certificación (*art. 42 y 43*).
 - Autoridades de control (*art. 41.4*).

- Máximo de (la cuantía más alta):
- **10 000 000 €**
 - **2 % del vol. fact. anual**

MUY GRAVES

- Principios básicos del tratamiento (*art. 5, 6, 7 y 9*).
- Derechos de los interesados (*art. 12 a 22*).
- Transferencias internacionales (*art. 44 a 49*).

- Máximo de (la cuantía más alta):
- **20 000 000 €**
 - **4 % del vol. fact. anual**

LEVES

- Artículo 74*
- Principio de transparencia.
 - Desatención derechos de los interesados.
 - No facilitar datos de contacto, etc.

Hasta 40 000 €

GRAVES

- Artículo 73*
- Tratar datos de menores sin consentimiento
 - Obstaculización derechos de los interesados.
 - Contratación de encargados por otro encargado sin autorización del responsable, etc.

40 001 € - 300 000 €

MUY GRAVES

- Artículo 72*
- Principios básicos del tratamiento
 - Utilizar los datos para una finalidad no compatible para la que fueron recogidos.
 - Vulnerar la confidencialidad, etc.

- Máximo de (la cuantía más alta):
- **20 000 000 €**
 - **4 % del vol. fact. anual**

LOPD

Infracciones y sanciones

Administración pública no proceden sanciones económicas

Cuando una AAPP comete alguna infracción, la AEPD dictará resolución declarando la infracción y estableciendo:



Las **medidas para el cese** de la conducta



La **corrección de los efectos** de la infracción



Acciones disciplinarias cuando existan indicios suficientes



Cuando las infracciones sean imputables a autoridades y directivos, en la resolución se incluirá una amonestación, con denominación del cargo responsable, y se ordenará la publicación en el BOE o en el BOJA.



Publicación en la web de la AEPD de la identidad del responsable que hubiera cometido la infracción (daño reputacional).

Comparativa de incremento de sanciones del RGPD vs LOPD



Infracciones y sanciones

Mayores sanciones

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	
ETid-1844	IRELAND	2023-05-12	1,200,000,000	Meta Platforms Ireland Limited	Art. 46 (1) GDPR	Insufficient legal basis for data processing	link link
ETid-778	LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.	Unknown	Non-compliance with general data processing principles	link
ETid-1373	IRELAND	2022-09-05	405,000,000	Meta Platforms, Inc.	Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 24 GDPR, Art. 25 (1), (2) GDPR, Art. 35 GDPR	Non-compliance with general data processing principles	link link
ETid-1543	IRELAND	2023-01-04	390,000,000	Meta Platforms Ireland Limited	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR	Non-compliance with general data processing principles	link
ETid-2032	IRELAND	2023-09-01	345,000,000	TikTok Limited	Art. 5 (1) c), 5 (1) f) GDPR, Art. 12 (1) GDPR, Art. 13 (1) e) GDPR, Art. 24 (1) GDPR, Art. 25 (1), (2) GDPR	Non-compliance with general data processing principles	link
ETid-2447	THE NETHERLANDS	2024-07-22	290,000,000	Uber Technologies Inc., Uber B.V.	Art. 44 GDPR	Non-compliance with general data processing principles	link link
ETid-1502	IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited	Art. 25 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link link

Infracciones y sanciones

Mayores sanciones en España

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
<input type="text" value="Filter Column"/>	<input type="text" value="spain"/>		<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	
ETid-1176	SPAIN	2022-05-18	10,000,000	Google LLC	Art. 6 GDPR, Art. 17 GDPR	Insufficient legal basis for data processing	link
ETid-594	SPAIN	2021-03-11	8,150,000	Vodafone España, S.A.U.	Art. 28 GDPR, Art. 24 GDPR, Art. 44 GDPR, Art. 21 LSSI, Art. 48 (1) b) LGT, Art. 21 GDPR, Art. 23 LOPDGDD	Insufficient fulfilment of data subjects rights	link
ETid-2220	SPAIN	2023-10-25	6,100,000	ENDESA ENERGÍA, S.A.U.	Art. 5 (1) f) GDPR, Art. 32 GDPR, Art. 33 GDPR, Art. 34 GDPR, Art. 44 GDPR	Non-compliance with general data processing principles	link
ETid-522	SPAIN	2021-01-13	6,000,000	Caixabank S.A.	Art. 6 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient legal basis for data processing	link
ETid-2216	SPAIN	2023-10-26	5,000,000	CAIXABANK, S.A.	Art. 5 (1) f) GDPR, Art. 25 GDPR, Art. 32 GDPR	Non-compliance with general data processing principles	link
ETid-481	SPAIN	2020-12-11	5,000,000	Banco Bilbao Vizcaya Argentaria, S.A.	Art. 6 GDPR, Art. 13 GDPR	Insufficient fulfilment of information obligations	link
ETid-1055	SPAIN	2022-02-01	3,940,000	Vodafone España, S.A.U.	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR	Non-compliance with general data processing principles	link
ETid-884	SPAIN	2021-10-21	3,000,000	CAIXABANK PAYMENTS & CONSUMER EFC, EP, S.A.U.	Art. 6 (1) GDPR	Insufficient legal basis for data processing	link
ETid-777	SPAIN	2021-07-26	2,520,000	Mercadona S.A.	Art. 5 (1) c) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 25 (1) GDPR, Art. 35 GDPR	Insufficient legal basis for data processing	link
ETid-2201	SPAIN	2023-07-28	2,500,000	Open Bank, S.A.	Art. 25 GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link

Infracciones y sanciones



Artículo 77 - 84

La transferencia de datos a otros países de la UE se podrá realizar si hay consentimiento expreso del interesado, la transferencia es afín a la finalidad del tratamiento y existen garantías de seguridad.

Proceso disciplinario

La normativa de protección de datos FGUCM indica que si un usuario no observe los preceptos señalados en dicha normativa, sin perjuicio de las acciones disciplinarias y administrativas y las responsabilidades legales, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.

Usuarios finales

Deben comunicar inmediatamente cualquier conocimiento de incumplimiento con el fin de solventarlo a la mayor brevedad.



Implicaciones ENS



- **Art. 3.1 ENS** indica que cuando un sistema trate datos personales se aplicarán las medidas de la LOPDGDD, del resto de normativa de aplicación, así como los criterios que se establezcan por la AEPD, sin perjuicio de los requisitos establecidos en el presente real decreto.

ENS: artículo 3.1



LOPD

Garantía de los Derechos Digitales

Garantía de los Derechos Digitales

Apartado específico de la LOPDGDD Título X

Artículo 87

Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

Derecho a la intimidad en el uso de los dispositivos corporativos.

El empleador podrá acceder a los contenidos solo para:

- Controlar el cumplimiento de las obligaciones laborales.
- Garantizar la integridad de los dispositivos.

Se deberán establecer criterios de utilización de los dispositivos (buenas prácticas).

Artículo 88

Derecho a la desconexión digital en el ámbito laboral

Los trabajadores tendrán derecho a la desconexión fuera del horario de trabajo:

- Respeto de su tiempo de descanso.
- Permisos y vacaciones.
- Su intimidad personal y familiar.

Artículo 89

Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

Se debe informar a los trabajadores si van a ser grabados por videovigilancia. No se pueden instalar cámaras en lugares como vestuarios, aseos, comedores y análogos.

Deber de respeto al principio de proporcionalidad e intervención mínima.



Buenas Prácticas

Decálogo de buenas prácticas

Buenas prácticas generales **RGPD y ENS**

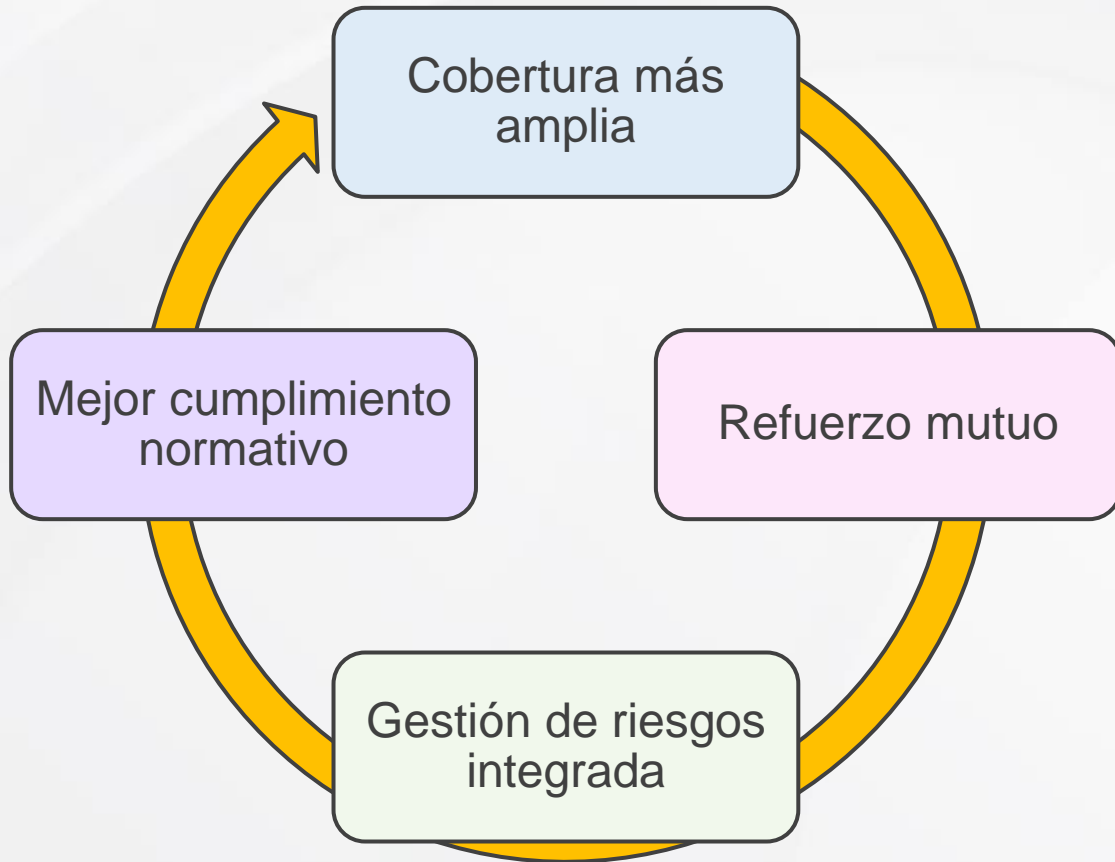
1. Evaluación de riesgos permanente: los riesgos se gestionan de forma continua.
2. Desarrollar y documentar políticas de seguridad y protección de datos.
3. Control de acceso basado en la necesidad.
4. Medidas técnicas de seguridad apropiadas (cifrado, seudonimización y control de accesos).
5. Tener bien definido el procedimiento de gestión de incidentes y notificaciones a las autoridades de control.
6. Auditorías y revisión continua.
7. Formación y concienciación del personal.
8. Gestión de proveedores y de la cadena de suministro.
9. EIPDs y clasificación de activos (ayuda a que los riesgos se identifiquen y gestionen de manera oportuna).
10. Garantía de Confidencialidad, Integridad y Disponibilidad



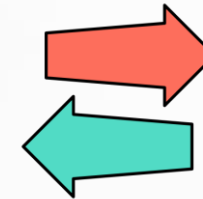
Conclusiones

Conclusiones

Tanto el RGPD como el ENS tienen objetivos y se complementan entre sí, lo que garantiza:



La interacción entre el RGPD y el ENS fortalece la **seguridad de la información**, fomenta una cultura de protección proactiva y ayuda a mitigar riesgos.



Muchas gracias por su atención

BABEL