

# GESTIÓN DE LA INFORMACIÓN

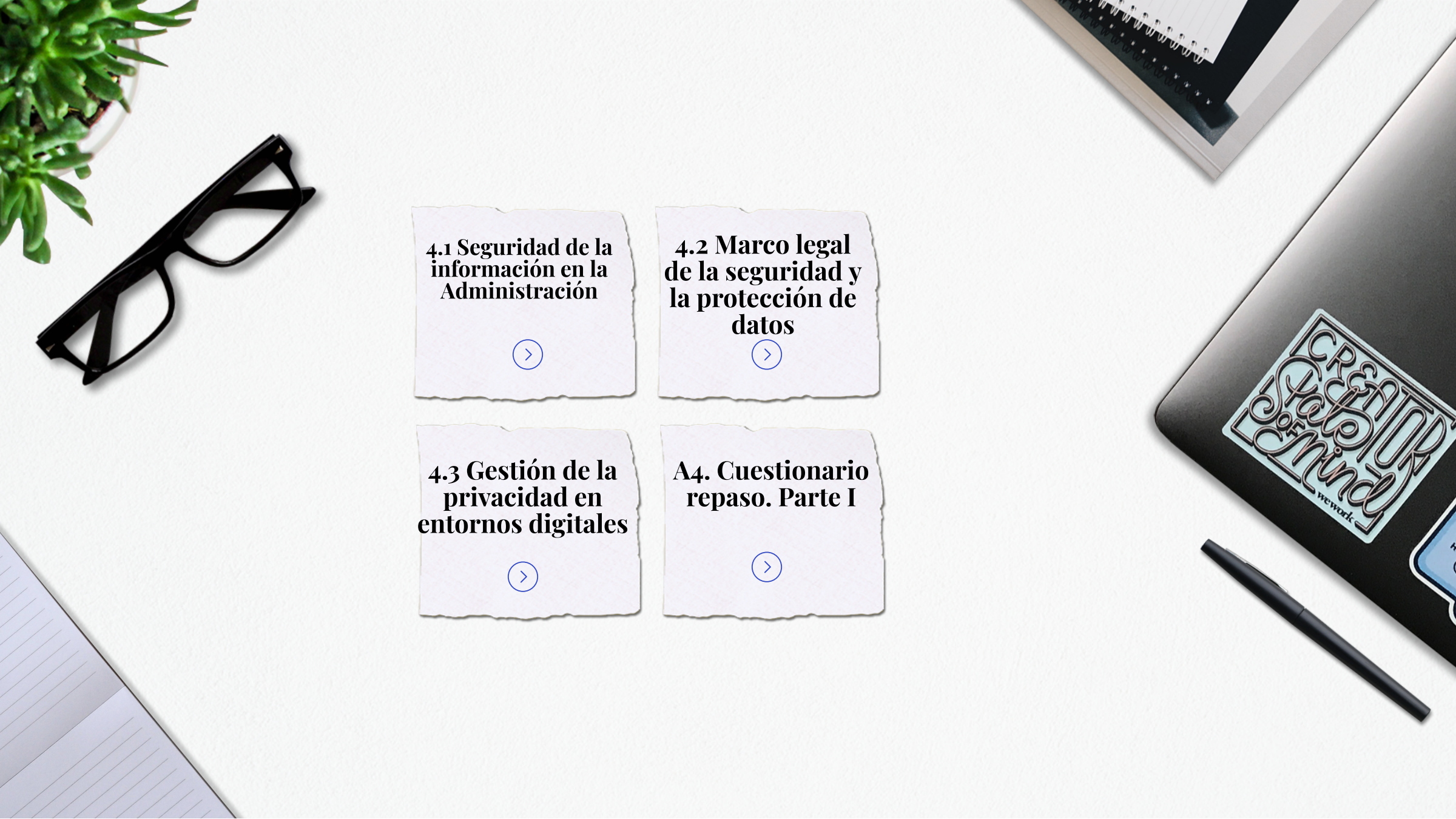
Curso 2025/2026

## UD 4: SEGURIDAD Y PRIVACIDAD (Parte I)



2º Grado Gestión y Administración Pública  
Prof. Ignacio Díaz Cano





**4.1 Seguridad de la  
información en la  
Administración**



**4.2 Marco legal  
de la seguridad y  
la protección de  
datos**



**4.3 Gestión de la  
privacidad en  
entornos digitales**



**A4. Cuestionario  
repaso. Parte I**





## 4.1 Seguridad de la información en la Administración

Protección de la información es una cuestión técnica y legal

garantizar



Organismos gubernamentales

gestionan

Seguridad es de importancia máxima en las AA.PP.

Datos sensibles de ciudadanos, empresas e infraestructuras críticas

Mecanismos básicos de la seguridad de la información en la administraciones

+ 4.1.1 PRINCIPIOS BÁSICOS DE LA SEGURIDAD Y LA PRIVACIDAD

+ 4.1.2 AMENAZAS COMUNES

+ 4.1.3 HERRAMIENTAS DE SEGURIDAD



## 4.1.1 Principios básicos de la seguridad y la privacidad

**Definición:** asegura que la información solo sea accesible por personas, entidades o sistemas autorizados.

**Ejemplo en la administración:** garantizar que los datos fiscales de un ciudadano solo estén disponibles para el personal autorizado de la Agencia Tributaria.

**Mecanismos:** control de accesos, autenticación robusta, cifrado.

**Definición:** implica que la información no pueda ser alterada de manera indebida, accidental o maliciosa.

**Ejemplo:** evitar que un expediente electrónico sea manipulado sin dejar trazabilidad.

**Mecanismos:** sumas de verificación, firmas digitales, sistemas de control de versiones.



triada CID

**Definición:** trata de que la información y los servicios deben estar accesibles cuando se necesitan.

**Ejemplo:** mantener operativos los portales de trámites electrónicos 24/7 para los ciudadanos.

**Mecanismos:** redundancia de sistemas, planes de contingencia, centros de respaldo.



## 4.1.2 Amenazas comunes

Tipos de ataques



Malware

- **Definición:** programas diseñados para dañar sistemas, robar datos o interrumpir servicios.

- **Tipos:** virus (comportamientos no deseados de los sistemas informáticos), gusanos (ralentizan el sistema), troyanos (los hackers pueden tomar el control del sistema), ransomware (encriptan la información).

- **Ejemplo:** ataques de ransomware a ayuntamientos europeos que han bloqueado sus sistemas de gestión tributaria.

Acceso no autorizado

- **Definición:** ocurre cuando personas o sistemas sin los permisos adecuados logran penetrar en redes gubernamentales.

**Riesgo:** robo de expedientes electrónicos, manipulación de datos o filtraciones masivas.

**Medidas:** autenticación multifactor, políticas de contraseñas, monitorización continua.

Phishing

- **Definición:** técnica de ingeniería social que consiste en el envío de correos electrónicos o mensajes fraudulentos que simulan ser de instituciones legítimas.

- **Objetivo:** engañar al usuario para que revele credenciales o datos bancarios.

- **Ejemplo:** correos falsos en nombre de la Seguridad Social solicitando actualización de datos.





## 4.1.3 Herramientas de seguridad

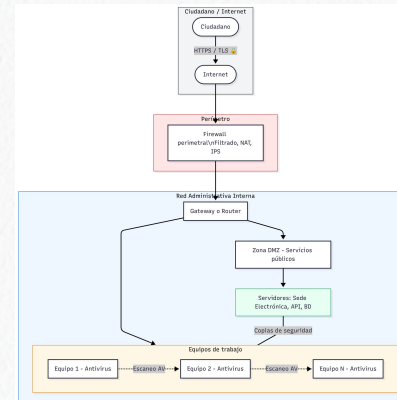


### Antivirus y antimalware

- **Definición:** software destinado a detectar, neutralizar y eliminar programas maliciosos
- **Uso en la administración:** proteger estaciones de trabajo de funcionarios y servidores que almacenan expedientes digitales.
- **Ejemplo:** detección temprana de ransomware en equipos de gestión documental.

### Firewalls (cortafuegos)

- **Definición:** dispositivos o programas que filtran el tráfico de red, permitiendo únicamente las comunicaciones autorizadas.
- **Uso en la administración:** segmentar redes internas, protegiendo sistemas sensibles como los registros civiles frente al acceso desde internet.
- **Tipos:** existen firewalls tradicionales (basados en reglas) y de nueva generación (con inspección profunda de paquetes).



### Cifrado

- **Definición:** técnica que convierte los datos en información ilegible para quien no disponga de la clave adecuada.
- **Uso en la administración:** comunicaciones cifradas entre ciudadanos y portales web (HTTPS), cifrado de bases de datos de padrones municipales.
- **Algoritmos habituales:** AES, RSA.



## 4.2 Marco legal de la seguridad y la protección de datos

AA.PP. españolas



Marco normativo  
multinivel

- Legislación europea
- Legislación estatal
- Estándares de seguridad

Base normativa

+ 4.2.1 RGPD

+ 4.2.2 LOPDGDD

+ 4.2.3 ENS



## 4.2.1 RGPD

Finalidad  
y ámbito

- Reglamento 2016/679 (RGPD).
- Obligatorio cumplimiento en todos los estados
- Regula tratamiento de datos personales por medio de entidades privadas y públicas
- RGPD en lo público

Principios  
y bases  
jurídicas

- Principios de licitud, lealtad, y transparencia
- Bases jurídicas: cumplimiento de una misión pública y cumplimiento de obligaciones legales

Derechos  
de las  
personas  
interesadas

- Derechos ARCO (acceso, rectificación, cancelación, oposición)
- Protección frente a decisiones automatizadas
- Responsable del tratamiento (art. 28)

Gobernanza y  
cumplimiento

Arts. relacionados  
Gestión Inf.

- Evaluaciones de impacto (EIPD): cuando se trata algo de riesgo (art. 35)
- Delegado Protección de Datos (DPD): obligada presencia en algunos casos (art. 37.1)
- Notificación brechas de seguridad a las autoridades (arts. 33-34)

+ 4.2.2 LOPDGDD

+ 4.2.3 ENS



## 4.2.2 Ley Orgánica de Protección de Datos y Derechos de Garantías Digitales (LOPDGDD)

Rol



LOPDGDD

- (L.O. 3/2018) de 5 de diciembre, adapta y complementa el RGPD en España
- Define particularidades del sector público,
- Regula aspectos concretos (videovigilancia)
- Consagra los derechos digitales en su Título X
- Edad mínima de 14 años para el consentimiento en servicios de la sociedad de la información



## 4.2.2 Ley Orgánica de Protección de Datos y Derechos de Garantías Digitales (LOPDGDD) (cont.)

Aspectos



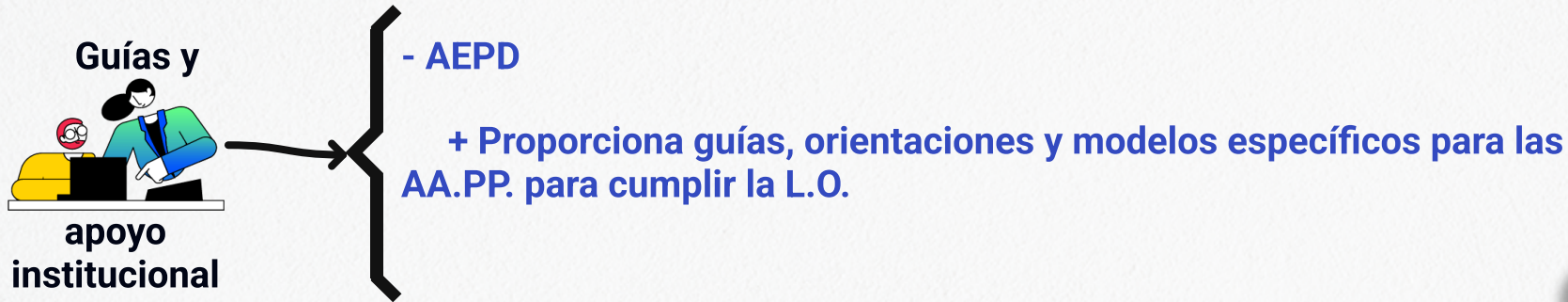
destacables  
para la AA.PP.

- Tratamientos con base en interés público
- Designación y funciones del DPD en AAPP
- Régimen de transparencia y acceso: coordinación con la normativa de transparencia
- Derechos digitales (Título X):
  - + Derecho a la seguridad digital
  - + Neutralidad de Internet
  - + Acceso universal
  - + Educación digital
  - + Desconexión digital en el ámbito laboral, entre otros.
- Régimen sancionador con graduación conforme a RGPD.





## 4.2.2 Ley Orgánica de Protección de Datos y Derechos de Garantías Digitales (LOPDGDD) (cont.)



Materia	RGPD (marco UE)	LOPDGDD (desarrollo España)
Obligación DPD	Autoridades u organismos públicos	Refuerzo del rol y relación con AEPD
Edad de consentimiento	No fija (corresponde a Estados 13-16)	<b>14 años</b>
Derechos digitales	No desarrolla catálogo específico	<b>Título X</b> (seguridad, educación, desconexión, etc.)
Tratamientos sectoriales	Principios y bases generales	Reglas y matices para empleo público, videovigilancia, etc.

Tabla 4.2: Comparativa entre RGPD y LOPDGDD en la Administración Pública



## 4.2.3 Esquema Nacional de Seguridad (ENS)

Naturaleza

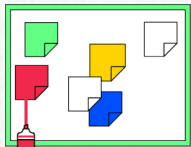


y objetivos

- Fija los principios básicos y requisitos mínimos que deben observar los sistemas que soportan servicios públicos y las entidades privadas que los prestan o mantienen.

- Principios, tales como: seguridad como proceso integral; prevención, detección y corrección; reevaluación periódica del riesgo.

Principios



medidas,  
conformidad

- Requisitos mínimos y medidas organizativas, operativas y de protección, con adecuación a categorías de seguridad del sistema (Bajo/Medio/Alto).

- Instrucciones Técnicas de Seguridad (ITS) de obligado cumplimiento, y guías CCN-STIC1 como apoyo a la implantación (p. ej., valoración de sistemas, ámbito de aplicación).

Funciones del Centro Criptológico Nacional Computer Emergency Response Team (CCN-CERT) como órgano de referencia técnica para el sector público.

- La LOPDGDD/ RGPD aseguran legalidad y derechos;

- El ENS asegura seguridad técnica y organizativa.

- Ambos planos se complementan, y deben integrarse en el denominado Sistema de Gestión de Seguridad (SGSI) de la entidad.



Índice



## 4.3 Gestión de la privacidad en entornos digitales

Gestión de la  
privacidad



en las AA.PP.

exige

- Integrar principios jurídicos y controles técnicos en todo el ciclo de vida del dato. Desde el diseño del trámite a la prestación del servicio y la eliminación de la información

- Esta gestión se apoya en tres pilares:

+ Consentimiento informado, si procede

+ Garantía efectiva de derechos

+ Medidas basadas en la prevención de riesgo



4.3.1 CONSENTIMIENTO  
INFORMADO



4.3.2 EVALUACIONES DE  
IMPACTO Y MEDIDAS  
PROACTIVAS



## 4.3.1 Consentimiento informado

### Concepto y requisitos de validez

"Consentimiento es la manifestación de la voluntad del ciudadano para el tratamiento de sus datos cuando la Administración no puede apoyarse en base jurídica".  
P.e. Consentimiento para comunicaciones adicionales

Consentimiento



para que  
sea válido

Informado

- Libre (sin coacciones ni condicionamientos indebidos; evitar "empaquetar" consentimientos).
- Específico (vinculado a finalidades determinadas, no genéricas).
- Informado (el interesado conoce quién trata sus datos, con qué fines, qué derechos tiene y cómo ejercerlos).
- Inequívoco (acción afirmativa clara: marcar una casilla, firmar digitalmente, etc.; no valen casillas premarcadas ni silencio).
- Granular (una opción por cada finalidad).
- Verificable (prueba del consentimiento).
- Revocable: con la misma facilidad con la que se otorgó.





## 4.3.1 Consentimiento informado

Prácticas recomendadas en sedes y apps públicas

Buenas



prácticas

- Capas informativas: un aviso breve (quién, para qué, derechos, enlace a info ampliada) + política completa accesible.
- Diseño sin “patrones oscuros”: evitar interfaces que induzcan a aceptar por defecto (p. ej., cookies no esenciales).
- Gestión de cookies: separar cookies técnicas (no requieren consentimiento) de analíticas/marketing (requieren consentimiento explícito en entornos públicos).
- Consentimiento de menores: reforzar la autenticación/representación cuando proceda; controles parentales en servicios educativos.
- Registro de evidencias: sellado temporal del consentimiento, logs y versión del texto mostrado.





## 4.3.1 Consentimiento informado

Derechos ARCO

**Acceso:** conocer si se tratan sus datos y obtener copia e información asociada (finalidades, categorías, cesiones, plazos, etc.).

**Rectificación:** corregir datos inexactos o incompletos.

**Cancelación/Supresión:** eliminación cuando ya no sean necesarios, el ciudadano retire el consentimiento o exista obligación legal de suprimir.

**Oposición:** oponerse al tratamiento en determinadas circunstancias (especialmente tratamientos no necesarios para el servicio público concreto).



**Extensión en el marco actual:** además de ARCO, el marco vigente reconoce limitación del tratamiento, portabilidad y no ser objeto de decisiones automatizadas. En entornos públicos, la oposición y la supresión pueden estar limitadas por obligaciones legales o por el interés público prevalente, pero el organismo debe motivar y documentar dichas limitaciones.





## 4.3.1 Consentimiento informado

### Gestión operativa en Administraciones Públicas

#### Principios



AA.PP.

- *Canales accesibles*: sede electrónica, oficinas de registro, y canal del DPD (Delegado/a de Protección de Datos).
- *Autenticación robusta*: identificación mediante certificados, sistemas clave PIN, o equivalentes para evitar entrega a terceros.
- *Plazos de respuesta*: procedimientos internos que aseguren la respuesta en plazo legal, con posibilidad de ampliación motivada en casos complejos.
- *Trazabilidad*: registro de solicitudes, decisiones, fechas, personas responsables y documentación entregada.
- *Interacción con terceros*: si existen encargados del tratamiento, establecer flujos para recuperar/bloquear/suprimir en sus sistemas.
- *Excepciones motivadas*: cuando prevalezcan obligaciones legales (p. ej., conservación por archivo público o procedimiento judicial).



4.3.2 EVALUACIONES DE  
IMPACTO Y MEDIDAS  
PROACTIVAS



## 4.3.2 Evaluaciones de impacto y medidas proactivas

Enfoque de riesgo

responsabilidad proactiva



exige que la organización que demuestre el cumplimiento

- *Privacy by design*: integrar la privacidad desde el inicio del proyecto (p. ej., minimización de datos, seudonimización, partición de finalidades, controles de acceso).
- *Privacy by default*: la configuración por defecto debe ser la más protectora (p. ej., desactivar por defecto analíticas no esenciales).
- Inventario de tratamientos: registro actualizado con finalidades, bases jurídicas, categorías de datos, cesiones, plazos y medidas.
- Gobernanza: roles claros (Responsable, Encargado, DPD), políticas, formación y auditorías.





## 4.3.2 Evaluaciones de impacto y medidas proactivas

### Evaluaciones de Impacto en Protección de Datos (EIPD)

Una EIPD es obligatoria cuando un tratamiento pueda implicar alto riesgo para los derechos y libertades (p. ej., evaluación sistemática y extensa, uso de categorías especiales de datos, biometría, etc.)..

#### Fases típicas



- *Descripción sistemática del tratamiento:* finalidad, contexto, datos, actores, ciclo de vida.
- *Necesidad y proporcionalidad:* base jurídica, idoneidad y alternativas menos intrusivas.
- *Análisis de riesgos:* identificación de amenazas, probabilidad/impacto, escenarios de abuso o error.
- *Medidas previstas:* técnicas (cifrado, seudonimización, control de accesos, retención) y organizativas (políticas, formación, auditoría).
- *Resultado:* riesgo residual aceptable o consulta previa a la autoridad de control si persiste el alto riesgo.
- *Plan de revisión:* reevaluación periódica o ante cambios sustantivos (nuevas finalidades, nuevas fuentes de datos, IA, etc.).





## 4.3.2 Evaluaciones de impacto y medidas proactivas

### Catálogo de medidas proactivas

*Minimización:* recoger solo los datos necesarios para cada finalidad.

*Seudonimización/Anonimización:* reducir el vínculo directo con el interesado en analítica o publicación de datos abiertos.

*Retención y borrado:* calendarios de conservación con bloqueo cuando lo exija el archivo público.

*Transparencia:* panel de privacidad en la sede electrónica con estado de consentimientos, bases jurídicas y derechos.

*Seguridad:* cifrado en tránsito y reposo; autenticación multifactor para perfiles con acceso a expedientes; registro y correlación de eventos.

*Evaluación de terceros:* cláusulas y auditorías a encargados y proveedores cloud (transferencias internacionales, subencargados, certificaciones).

*Formación y cultura:* programas periódicos, simulacros (p. ej., phishing), métricas de madurez.





# GESTIÓN DE LA INFORMACIÓN

Curso 2025/2026

## UD 4: SEGURIDAD Y PRIVACIDAD (Parte I)



[+ IR A PARTE II](#)

2º Grado Gestión y Administración Pública  
Prof. Ignacio Díaz Cano

[+ A.4 CUESTIONARIO  
PARTE I](#)





## A4 Cuestionario Repaso. Parte I

1. ¿Cuál de los siguientes principios forma parte de la tríada básica de la seguridad de la información (CID)?:

Confidencialidad

Transparencia

Neutralidad de red

Legalidad

Send



Índice





## A4 Cuestionario Repaso. Parte I

2. ¿Qué se entiende por “integridad” en el contexto de la seguridad de la información?:

Que solo sea accesible para usuarios autorizados

Que la información no sea alterada indebidamente

Que la información esté cifrada permanentemente

Que la información esté siempre disponible

Send



Índice





## A4 Cuestionario Repaso. Parte I

3. ¿Cuál de las siguientes amenazas se caracteriza por engañar al usuario mediante correos o mensajes falsos?:

Ransomware

Phishing

Troyano

Spyware

Send



Índice





## A4 Cuestionario Repaso. Parte I

4. ¿Qué objetivo tiene el cifrado en la administración pública?:

Convertir los datos en información ilegible para quien no tenga la clave

Sustituir la autenticación multifactor

Evitar errores administrativos

Garantizar la rapidez en la transmisión de datos

Send



Índice





## A4 Cuestionario Repaso. Parte I

5. ¿Qué norma europea regula el tratamiento de datos personales en todos los Estados miembros de la UE?:

LOPDGDD

ENS

ISO/IEC 27001

RGPD

Send



Índice





## A4 Cuestionario Repaso. Parte I

6. Según la LOPDGDD, ¿cuál es la edad mínima para prestar consentimiento en servicios de la sociedad de la información en España?:

14 años

18 años

13 años

16 años

Send



Índice





## A4 Cuestionario Repaso. Parte I

7. ¿Qué organismo proporciona guías y modelos para el cumplimiento de la LOPDGDD en la Administración Pública?:

AEPD

CCN-CERT

ENISA

INCIBE

Send



Índice





## A4 Cuestionario Repaso. Parte I

8. El Esquema Nacional de Seguridad (ENS) está regulado por:

El Reglamento General de Protección de Datos

El Reglamento (UE) 2016/679

La Ley Orgánica 3/2018

El Real Decreto 311/2022

Send



Índice





## A4 Cuestionario Repaso. Parte I

9. ¿Cuál de las siguientes condiciones NO es requisito de validez del consentimiento informado?:

Ser informado

Ser verificable

Ser implícito

Ser libre

Send



Índice





## A4 Cuestionario Repaso. Parte I

10. ¿Qué principio describe la integración de la privacidad desde el diseño de los sistemas y servicios?:

Accountability

Privacy by design

Security by default

Data protection impact

Send



Índice

