

Persevera

AL ALCANCE DE QUIEN ESTUDIA

Tema 17

Tecnologías de la información y la comunicación

Guardia Civil · Escala de Cabos y Guardias

ACCESO DIRECTO · EDICIÓN 2026

perseveraoposiciones.com

AL ALCANCE DE QUIEN ESTUDIA

Cada año, mucha gente perfectamente capaz de aprobar una oposición no llega a intentarlo en serio. Y casi nunca es por falta de cabeza: es por la vida. El trabajo que te deja sin fuerzas justo cuando ibas a ponerte, las cargas familiares, no saber bien por dónde empezar o, simplemente, no poder dedicarle el día entero ni pagar una buena academia. Cosas que poco tienen que ver con lo que uno valdría sentado delante del examen.

Persevera nace de ahí: de la idea de que opositar debería depender de que estudies, y de nada más.

Prepararse bien no debería depender de cosas ajenas a tu esfuerzo. Hay muchísima gente que sacaría la plaza por su cuenta si tuviera las herramientas adecuadas a mano. El problema es que casi siempre se ven solo dos caminos: una academia, con sus horarios y su ritmo, o hacerlo del todo en solitario, sin nada ni nadie que te guíe. Persevera quiere ser un tercer camino: la libertad de ir por tu cuenta, pero con herramientas de verdad para hacerlo en serio.

Ese tercer camino empieza por lo esencial: el temario, completo y gratuito, sin registrarte. Descárgalo, guárdalo, imprímelo, compártelo con quien quieras: es tuyo, sin compromisos y para siempre.

Y las herramientas de verdad están en nuestra app. Porque, como quienes hemos pasado por ahí, sabemos que tener el temario es solo el principio: en la app el temario cobra vida, con tests para ponerte a prueba, fichas de repaso, esquemas y un seguimiento que te muestra por dónde vas y dónde flojeas. Todo pensado para exprimir cada hora de estudio. Y da lo mismo cómo te prepares: por tu cuenta o como refuerzo de una academia, aquí siempre tienes con qué practicar más.

Opositar es, sobre todo, perseverar: madrugones, días en que no entra nada, semanas en que dudas de si merece la pena. Y es en esa parte —la de aguantar— donde queremos estar a tu lado, dándote las herramientas que a nosotros nos habrían hecho el camino más fácil.

— *El equipo de Persevera*

ÍNDICE

Epígrafe 1 — Los sistemas de telecomunicaciones y las TIC en la Administración General del Estado	5
1. Dos planos normativos que conviene no confundir	5
2. Ley 11/2022 General de Telecomunicaciones: objeto y ámbito	6
3. Salvaguardia de derechos fundamentales: secreto de las comunicaciones y protección de datos	9
4. RD 806/2014: el modelo de gobernanza de las TIC en la AGE	10
5. Los órganos y las palancas de la gobernanza TIC	12
Epígrafe 2 — Las técnicas criptográficas y los servicios electrónicos de confianza	15
1. La criptografía como fundamento técnico	15
2. La firma electrónica: simple, avanzada y cualificada	16
3. La Ley 6/2020: objeto y ámbito de aplicación	17
4. Los certificados electrónicos	19
5. El Documento Nacional de Identidad electrónico y sus certificados	20
6. Las obligaciones de los prestadores de servicios de confianza	21
Epígrafe 3 — La ciberseguridad: principios y recomendaciones básicas	24
1. El CCN-CERT y el enfoque de las recomendaciones básicas	24
2. La Internet profunda: web superficial, <i>deep web</i> y <i>dark web</i>	26
3. Navegación segura	27
4. Seguridad del correo electrónico: el <i>phishing</i>	28
5. Virtualización	28
6. Seguridad en dispositivos móviles y redes inalámbricas (wifi)	29
7. Mensajería instantánea y redes sociales	29

8. El Internet de las cosas (IoT)	30
Epígrafe 4 — El Esquema Nacional de Interoperabilidad	31
1. Objeto y ámbito de aplicación	31
2. Los principios básicos del Esquema Nacional de Interoperabilidad	33
3. Las dimensiones de la interoperabilidad	34
4. Las normas técnicas de interoperabilidad y su relación con el ENS	36
5. La reutilización y el licenciamiento de las aplicaciones	37
6. La conservación y recuperación del documento electrónico	38

TEMA 17

Epígrafe 1 — Los sistemas de telecomunicaciones y las TIC en la Administración General del Estado

1. Dos planos normativos que conviene no confundir

Este epígrafe cruza dos normas que operan en planos distintos, aunque ambas giran en torno a la tecnología de las comunicaciones:

- **La Ley 11/2022, de 28 de junio, General de Telecomunicaciones (LGTel)**, que regula el **sector** de las telecomunicaciones: la instalación y explotación de redes, la prestación de servicios de comunicaciones electrónicas, el dominio público radioeléctrico y los equipos. Es la norma de cabecera del mercado, dictada al amparo del art. 149.1.21.^a CE (competencia estatal exclusiva).
- **El Real Decreto 806/2014, de 19 de septiembre**, que no regula el sector, sino la **organización interna** de las Tecnologías de la Información y las Comunicaciones (TIC) dentro de la Administración General del Estado: cómo se gobierna, planifica y coordina la Administración digital puertas adentro.

La primera mira hacia el mercado y los operadores; la segunda, hacia la propia máquina administrativa. El punto de contacto es que la AGE es, a la vez, reguladora del sector y una gran organización que consume y gobierna sus propios sistemas TIC.

MATIZ

La LGTel se dicta ex art. 149.1.21.^a CE («régimen general de comunicaciones (...) correos y telecomunicaciones»), competencia **exclusiva** del Estado. El RD 806/2014, en cambio, es una norma de autoorganización que la AGE se da a sí misma: no crea derechos ni obligaciones frente a los operadores, sino que ordena la gobernanza TIC entre ministerios y organismos públicos.

2. Ley 11/2022 General de Telecomunicaciones: objeto y ámbito

El **Título I** de la Ley agrupa las disposiciones generales. Su artículo 1 fija qué regula la ley y qué queda fuera de ella.

Artículo 1 · Objeto y ámbito de aplicación

1. El objeto de esta ley es la **regulación de las telecomunicaciones**, que comprende la instalación y explotación de las **redes de comunicaciones electrónicas**, la prestación de los **servicios de comunicaciones electrónicas**, sus recursos y servicios asociados, los **equipos radioeléctricos** y los **equipos terminales de telecomunicación**, de conformidad con el **artículo 149.1.21.^a de la Constitución**.

En particular, esta ley es de aplicación al **dominio público radioeléctrico** utilizado por parte de todas las redes de comunicaciones electrónicas, ya sean públicas o no, y con independencia del servicio que haga uso del mismo.

2. Quedan **excluidos** del ámbito de esta ley los **servicios de comunicación audiovisual**, los servicios de intercambio de vídeos a través de plataforma, los contenidos audiovisuales transmitidos a través de las redes, así como el régimen básico de los medios de comunicación social de naturaleza audiovisual a que se refiere el **artículo 149.1.27.^a de la Constitución**.

Asimismo, se excluyen del ámbito de esta ley los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas, las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos y los **servicios de la Sociedad de la Información**, regulados en la **Ley 34/2002, de 11 de julio**, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en tanto en cuanto no sean asimismo servicios de comunicaciones electrónicas.

Junto al objeto, el Título I fija dos ideas rectoras que conviene retener:

- **Las telecomunicaciones son servicios de interés general prestados en régimen de libre competencia** (art. 2.1). Solo tienen la consideración de **servicio público** o quedan sujetos a **obligaciones de servicio público** los supuestos tasados del art. 4 y del Título III, respectivamente (art. 2.2).
- El **art. 3** enumera los objetivos y principios de la ley: fomentar la competencia efectiva, desarrollar la economía y el empleo digital, impulsar el despliegue de redes de muy alta capacidad, garantizar el servicio universal y contribuir al mercado interior europeo de comunicaciones electrónicas, entre otros.

MATIZ

La clave del ámbito está en la frontera con lo audiovisual y con la Sociedad de la Información: los contenidos y el control editorial quedan **fuera** lo que la ley regula es el «continente» (redes, servicios de transporte, espectro, equipos), no el «contenido». Un mismo prestador puede estar dentro por su faceta de comunicaciones electrónicas y fuera por su faceta de contenidos.

El **art. 3** merece leerse en su literalidad, porque el examen pregunta objetivos concretos —en especial la letra e), que el resumen anterior no recoge—.

Artículo 3 · Objetivos y principios de la ley (extracto)

Los objetivos y principios de esta ley son los siguientes:

- a) fomentar la competencia efectiva y sostenible en los mercados de telecomunicaciones (...);
- b) desarrollar la economía y el empleo digital, promover el desarrollo del sector de las telecomunicaciones (...);
- e) **promover el desarrollo de la ingeniería, así como de la industria de productos y equipos de telecomunicaciones**

f) contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea (...).

Junto a los objetivos, el **art. 4** reserva la condición de **servicio público** a los servicios de telecomunicaciones para la seguridad nacional, la defensa, la seguridad pública, la seguridad vial y la protección civil. Su apartado 5 precisa quién fija las medidas de seguridad de las infraestructuras.

Artículo 4.5 · Medidas de seguridad de los bienes afectos a las redes

5. Los bienes muebles o inmuebles vinculados a los centros, establecimientos y dependencias afectos a la instalación y explotación de las redes y a la prestación de los servicios de comunicaciones electrónicas dispondrán de las medidas y sistemas de seguridad, vigilancia, difusión de información, prevención de riesgos y protección que se determinen por **el Gobierno**, a propuesta de los Ministerios de Defensa, del Interior o de Asuntos Económicos y Transformación Digital, dentro del ámbito de sus respectivas competencias.

RECUERDA

Dos ganchos del Título I de la LGTel: entre los objetivos del **art. 3** figura «**promover el desarrollo de la ingeniería, así como de la industria de productos y equipos de telecomunicaciones**» (letra e); y las medidas de seguridad y vigilancia de los **bienes muebles o inmuebles afectos** a las redes las determina **el Gobierno** (art. 4.5), a propuesta de Defensa, Interior o Asuntos Económicos y Transformación Digital.

3. Salvaguardia de derechos fundamentales: secreto de las comunicaciones y protección de datos

Dentro del **Título III**, el **Capítulo III** se rubrica «Salvaguardia de derechos fundamentales, secreto de las comunicaciones y protección de los datos personales». Es la sede donde la ley conecta la actividad de los operadores con los derechos del art. 18 CE.

El **art. 56** abre el capítulo con la **salvaguardia de los derechos fundamentales**: cualquier medida que restrinja el acceso o el uso de servicios y aplicaciones a través de redes de comunicaciones electrónicas solo podrá imponerse si es **adecuada, necesaria y proporcionada** en una sociedad democrática, con las debidas salvaguardias de procedimiento (presunción de inocencia, intimidad, libertad de expresión, tutela judicial efectiva). El **art. 57** añade el **principio de no discriminación** por nacionalidad, residencia o lugar de establecimiento del usuario final, salvo justificación objetiva.

El núcleo del capítulo es el art. 58, que impone a los operadores el deber de garantizar el secreto de las comunicaciones y de colaborar con las interceptaciones legales.

Artículo 58 · Secreto de las comunicaciones

1. Los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán **garantizar el secreto de las comunicaciones** de conformidad con los **artículos 18.3 y 55.2 de la Constitución**, debiendo adoptar las **medidas técnicas necesarias**.
2. Los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones interpersonales basados en numeración disponibles al público o servicios de acceso a internet están obligados a realizar las **interceptaciones que se autoricen judicialmente** de acuerdo con lo establecido en el capítulo V del título VIII del libro II de la **Ley de Enjuiciamiento Criminal**, en la **Ley Orgánica 2/2002, de 6 de mayo**, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica.

Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

Los apartados 3 a 11 del art. 58 descienden al detalle técnico de esa obligación: precisan sobre qué comunicaciones y terminales recae la interceptación (ap. 3 y 4), qué **datos** debe facilitar el operador al agente facultado —identidades, servicios utilizados, marcas temporales, información de localización, etc. (ap. 5 a 7)—, la regla de que solo se entrega lo incluido en la **orden de interceptación legal** (ap. 8), la información previa sobre el sistema del sujeto vigilado (ap. 9), la exigencia de mantener **interfaces** de transmisión a los centros de recepción (ap. 10) y el deber de entregar las comunicaciones **descifradas** cuando la codificación sea reversible (ap. 11).

En el plano de los datos personales, el **art. 66** reconoce a los usuarios finales el **derecho a la protección de datos personales y a la privacidad** en relación con las comunicaciones, remitiéndose al RGPD (Reglamento (UE) 2016/679) y a la **LO 3/2018, de 5 de diciembre**, de Protección de Datos Personales y garantía de los derechos digitales, y atribuyendo a la **Agencia Española de Protección de Datos** la competencia de supervisión en este ámbito.

RECUERDA

El **secreto de las comunicaciones** (art. 58 LGTel) se ancla en los **arts. 18.3 y 55.2 CE**: es un deber de los operadores, garantizado con medidas técnicas, que **solo cede ante autorización judicial**. La interceptación se rige por la LECrim (cap. V, tít. VIII, libro II) y por la LO 2/2002 del control judicial previo del CNI. La protección de datos se remite al RGPD y a la LO 3/2018, bajo supervisión de la AEPD.

4. RD 806/2014: el modelo de gobernanza de las TIC en la AGE

Cambiamos de plano. El RD 806/2014 no mira al mercado, sino a la **organización interna** de la Administración digital. Su artículo 1 define con precisión qué persigue la norma.

MATIZ

El **RD 806/2014** fue **derogado** en su integridad por el **Real Decreto 1125/2024, de 5 de noviembre**, en vigor desde el **7 de noviembre de 2024**, que sustituye este modelo de gobernanza: crea la **Agencia Estatal de Administración Digital** (en lugar de la extinta Secretaría General de Administración Digital) y la **Comisión Estratégica de Tecnologías de la Información y las Comunicaciones (CETIC)**. Cuando el programa oficial siga citando el RD 806/2014, conviene estudiar su esquema teniendo presente que los órganos que se describen a continuación han quedado reemplazados por el nuevo modelo.

Artículo 1 · Objeto

El objeto de este real decreto es el **desarrollo y ejecución de un modelo común de gobernanza** de las **Tecnologías de la Información y las Comunicaciones (TIC)** en la **Administración General del Estado** y sus **Organismos Públicos**.

Este modelo de Gobernanza de las TIC incluirá, en todo caso, la definición e implementación de una **estrategia global de transformación digital** que garantice el uso adecuado de los recursos informáticos de acuerdo a las necesidades derivadas de la estrategia general del Gobierno, con el fin de **mejorar la prestación de los servicios públicos al ciudadano**.

El **ámbito de aplicación** (art. 2) se extiende a la **Administración General del Estado** y sus **Organismos Públicos** previstos en el art. 43 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la AGE (LOFAGE). La norma persigue tres ideas de fondo: **racionalizar** el gasto TIC, evitar **duplicidades** y **compartir** infraestructuras y servicios comunes en lugar de que cada ministerio actúe aislado.

5. Los órganos y las palancas de la gobernanza TIC

El modelo se articula en una **cadena de órganos** —del vértice político a la unidad de cada ministerio— y en un conjunto de **instrumentos** de planificación y coordinación.

Órgano / instrumento	Ubicación en el RD	Papel en la gobernanza
Comisión de Estrategia TIC	arts. 3-6	Órgano colegiado que define y supervisa la Estrategia TIC de la AGE; actúa en Pleno y por Comité Ejecutivo adscrita al entonces Ministerio de Hacienda y Administraciones Públicas
Comisiones Ministeriales de Administración Digital (CMAD)	art. 7	Órganos departamentales de impulso y coordinación interna; enlace de cada ministerio con la Dirección de TIC; presididas por el Subsecretario
Comité de Dirección de las TIC	art. 8	Órgano de apoyo adscrito a la Dirección de TIC; coordina metodologías, arquitecturas y buenas prácticas comunes entre unidades
Estrategia TIC	art. 9	Instrumento aprobado por el Gobierno , a iniciativa de la Comisión; fija objetivos, principios y acciones de la transformación digital
Medios y servicios compartidos	art. 10	Recursos TIC declarados de uso compartido por responder a necesidades transversales; la declaración corresponde a la Comisión de Estrategia TIC
Unidades TIC y cooperación interadministrativa	arts. 12-13	Estructuras técnicas de cada organismo y colaboración con CCAA y entidades locales

Las funciones de la **Comisión de Estrategia TIC** (art. 4) incluyen fijar las líneas estratégicas conforme a la política del Gobierno, aprobar la propuesta de Estrategia TIC para su elevación al Consejo de Ministros, informar anteproyectos y proyectos normativos en materia TIC, definir prioridades de inversión, **declarar medios o servicios compartidos** (art. 10) y **proyectos de interés prioritario** (art. 11), impulsar la cooperación con CCAA,

entidades locales y la Unión Europea, y actuar como **Observatorio de la Administración Electrónica y Transformación Digital**. La Comisión eleva, además, un **informe anual** al Consejo de Ministros sobre el estado de la transformación digital.

En el escalón departamental, las **CMAD** (art. 7) estudian y planifican las necesidades funcionales de cada ministerio, elaboran el **Plan de acción departamental para la transformación digital** (Cap. IV, arts. 14-15) y actúan como órgano de enlace con la Dirección de TIC, evitando duplicidades y promoviendo la compartición de servicios comunes. El **Capítulo V** (arts. 16-19) cierra el modelo con las actuaciones en materia de **contratación TIC**: el informe técnico sobre la memoria y los pliegos de prescripciones técnicas y la información presupuestaria asociada.

RECUERDA

La gobernanza TIC del RD 806/2014 se lee de arriba abajo: el **Gobierno** aprueba la **Estrategia TIC** → la **Comisión de Estrategia TIC** la define, supervisa y declara los **medios/servicios compartidos** → las **CMAD** la bajan a cada ministerio mediante sus **Planes de acción** → el **Comité de Dirección de las TIC** homogeneiza metodologías y buenas prácticas comunes. Objetivo transversal: racionalizar, compartir y evitar duplicidades.

El propio real decreto define en su **artículo 12** qué es una **unidad TIC** y qué funciones integran la «provisión de servicios TIC» —una lista cerrada que el examen usa para colar distractores como «consultoría telemática»—.

Artículo 12 · Unidades TIC

1. Son unidades TIC aquellas **unidades administrativas** cuya función sea la provisión de servicios en materia de Tecnologías de la Información y Comunicaciones **a sí mismas o a otras unidades administrativas**.
2. Se entenderá por provisión de servicios TIC la realización de una o varias de las siguientes funciones:

- a) Soporte, operación, implementación y/o gestión de sistemas informáticos corporativos o de redes de telecomunicaciones.
- b) Desarrollo de aplicativos informáticos en entornos multiusuario.
- c) Consultoría informática.
- d) Seguridad de sistemas de información.
- e) Atención técnica a usuarios.
- f) Innovación en el ámbito de las TIC
- g) Administración digital.
- h) Conformer la voluntad de adquisición de bienes o servicios en el ámbito de las tecnologías de la información y las comunicaciones
- i) Todas aquellas funciones no previstas expresamente en las letras anteriores, que sean relevantes en materia de tecnologías de la información y las comunicaciones.

RECUERDA

Una **unidad TIC** es una **unidad administrativa** —no «operativa»— que provee servicios TIC a **sí misma o a otras unidades administrativas** (art. 12.1). La «provisión de servicios TIC» comprende soporte y gestión de sistemas, **desarrollo de aplicativos, consultoría informática, seguridad de sistemas de información**, atención a usuarios, **innovación** y administración digital (art. 12.2). Trampa habitual: es «consultoría **informática**», no «consultoría telemática».

TEMA 17

Epígrafe 2 — Las técnicas criptográficas y los servicios electrónicos de confianza

Los servicios electrónicos de confianza —firma, sello, sellado de tiempo, certificados, autenticación de sitios web— descansan sobre una misma base técnica: la **criptografía**. Antes de abordar el régimen jurídico español (Ley 6/2020, complemento del Reglamento eIDAS), conviene fijar el marco conceptual que da sentido a certificados y firmas.

1. La criptografía como fundamento técnico

La **criptografía** es el conjunto de técnicas que transforman una información legible (texto en claro) en un formato ininteligible (texto cifrado o *criptograma*), de modo que solo quien posee la clave adecuada pueda recuperar el mensaje original. En el ámbito de la confianza electrónica persigue cuatro objetivos: **confidencialidad** (que solo el destinatario lea el mensaje), **integridad** (que no haya sido alterado), **autenticación** (certeza sobre el origen) y **no repudio** (que el emisor no pueda negar haber emitido el mensaje).

Según cómo se gestionen las claves, se distinguen dos grandes familias:

- **Criptografía simétrica (o de clave secreta)**: emisor y receptor comparten **una única clave**, que sirve tanto para cifrar como para descifrar. Es rápida y eficiente con grandes volúmenes de datos, pero plantea el problema de la **distribución segura de la clave**: hay que hacerla llegar al interlocutor por un canal seguro sin que un tercero la intercepte. Algoritmos característicos: AES, 3DES.
- **Criptografía asimétrica (o de clave pública)**: cada usuario dispone de un **par de claves** matemáticamente relacionadas —una **clave pública**, que difunde libremente, y una **clave privada**, que mantiene en secreto—. Lo cifrado con una de ellas solo puede descifrarse con la otra. Esto habilita dos usos complementarios:
 - **Confidencialidad**: el emisor cifra con la **clave pública** del destinatario; solo este, con su **clave privada**, puede descifrar.

- **Firma y autenticación:** el emisor cifra (firma) con su **clave privada** cualquiera puede verificarlo con la **clave pública** del emisor, lo que prueba el origen y la integridad.

Algoritmo característico: RSA. En la práctica se combina con **funciones hash o resumen**, que generan una «huella digital» de longitud fija del documento: la firma no cifra todo el texto, sino ese resumen, lo que hace el proceso más eficiente y permite detectar cualquier alteración posterior.

MATIZ

En la criptografía simétrica emisor y receptor comparten una misma clave secreta, lo que la hace rápida pero exige un canal seguro para intercambiarla. La asimétrica resuelve ese problema con un par de claves: lo cifrado con la pública solo se descifra con la privada, y a la inversa. La firma electrónica se apoya en la asimétrica —se firma con la clave privada y cualquiera verifica con la pública—.

2. La firma electrónica: simple, avanzada y cualificada

La **firma electrónica** aplica la criptografía asimétrica para vincular a una persona con un documento electrónico. El **Reglamento (UE) n.º 910/2014 (eIDAS)** —al que la Ley 6/2020 sirve de complemento— gradúa tres niveles de firma, de menor a mayor garantía:

Nivel	Rasgos esenciales	Valor jurídico
Firma electrónica (simple)	Datos en formato electrónico anejos o asociados a otros datos electrónicos que el firmante utiliza para firmar. Categoría más amplia (desde un nombre al pie de un correo hasta una casilla marcada).	No se le niegan efectos jurídicos ni valor probatorio por su mera forma electrónica.
Firma electrónica avanzada	Vinculada al firmante de manera única; permite identificarlo; creada con datos que el firmante puede utilizar bajo su control exclusivo vinculada a los datos firmados de modo que sea	Mayor fiabilidad; asegura identidad e integridad.

	detectable cualquier modificación posterior .	
Firma electrónica cualificada	Firma avanzada creada mediante un dispositivo cualificado de creación de firmas y basada en un certificado cualificado de firma electrónica.	Equivalente a la firma manuscrita (efecto jurídico equiparado).

La firma cualificada es, por tanto, la única a la que el Reglamento reconoce equivalencia plena con la firma de puño y letra, precisamente porque suma dos garantías adicionales sobre la avanzada: el dispositivo cualificado (por ejemplo, el chip del DNI electrónico o una tarjeta criptográfica) y el certificado cualificado expedido por un prestador de confianza.

RECUERDA

Tres niveles de firma electrónica en el marco eIDAS: **simple** (datos electrónicos que el firmante usa para firmar), **avanzada** (vinculada de forma única al firmante, bajo su control exclusivo y con integridad verificable) y **cualificada** (avanzada + dispositivo cualificado + certificado cualificado). Solo la cualificada se equipara a la firma manuscrita.

3. La Ley 6/2020: objeto y ámbito de aplicación

La norma española de cabecera es la **Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza**. No es una regulación autónoma y completa, sino un **complemento del Reglamento eIDAS**, de aplicación directa; además, su disposición derogatoria dejó sin efecto la anterior **Ley 59/2003, de 19 de diciembre, de firma electrónica**.

Artículo 1 · Objeto de la Ley

La presente Ley tiene por objeto **regular determinados aspectos de los servicios electrónicos de confianza**, como **complemento del Reglamento (UE) n.º 910/2014** del Parlamento Europeo y del Consejo, de 23 de julio de

2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

Artículo 2 · Ámbito de aplicación

Esta Ley se aplicará a los **prestadores públicos y privados** de servicios electrónicos de confianza **establecidos en España**.

Así mismo, se aplicará a los prestadores residentes o domiciliados en otro Estado que tengan un **establecimiento permanente situado en España**, siempre que ofrezcan servicios **no supervisados** por la autoridad competente de otro país de la Unión Europea.

En cuanto a los **efectos jurídicos**, el **artículo 3** dispone que los documentos electrónicos públicos, administrativos y privados tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza; y remite la prueba de los documentos electrónicos privados a los apartados 3 y 4 del artículo 326 de la Ley 1/2000, de Enjuiciamiento Civil, según se haya empleado un servicio de confianza no cualificado o cualificado.

MATIZ

La Ley 6/2020 no regula por sí sola los servicios de confianza: es complemento del Reglamento (UE) 910/2014 (eIDAS), de aplicación directa, y derogó la anterior Ley 59/2003 de firma electrónica. Solo desarrolla los aspectos que el Reglamento deja al Derecho nacional —vigencia de certificados, supervisión, régimen sancionador—, sin transponer nada, pues los reglamentos de la Unión no se transponen.

4. Los certificados electrónicos

Un **certificado electrónico** es el documento que un prestador de confianza expide para vincular unos datos de verificación de firma con una persona, confirmando su identidad. El **Título II** de la Ley regula su vigencia, extinción e identificación del titular. La norma nuclear sobre su duración es el artículo 4:

Artículo 4 · Vigencia y caducidad de los certificados electrónicos

1. Los certificados electrónicos se **extinguen por caducidad** a la expiración de su período de vigencia, o mediante **revocación** por los prestadores de servicios electrónicos de confianza en los supuestos previstos en el artículo siguiente.
2. El **período de vigencia de los certificados cualificados no será superior a cinco años**.

Dicho período se fijará en atención a las características y tecnología empleada para generar los datos de creación de firma, sello, o autenticación de sitio web.

El resto del Título II desarrolla las causas de extinción y las garantías de identidad:

- **Artículo 5 (revocación y suspensión)**: enumera los supuestos de **revocación** —entre otros, solicitud del firmante, puesta en peligro del secreto de los datos de creación de firma, resolución judicial o administrativa, fallecimiento o extinción de la personalidad jurídica del titular, cese del prestador, o falsedad de los datos aportados—. La **suspensión** procede en los casos de las letras a), c) y h) del apartado 1 y ante dudas sobre las letras b) y g), si así lo prevén las declaraciones de prácticas.
- **Artículo 6 (identidad y atributos)**: fija cómo se consigna la identidad del titular en los certificados cualificados —nombre y apellidos con DNI/NIE/NIF para personas físicas; denominación o razón social y NIF para personas jurídicas—, admitiendo el pseudónimo cuando conste como tal de forma inequívoca.
- **Artículo 7 (comprobación de la identidad)**: exige, con carácter general, la **personación** del solicitante ante los encargados de verificarla, acreditada mediante DNI,

pasaporte u otros medios admitidos en Derecho; admite prescindir de ella con firma legitimada notarialmente y regula la identificación a distancia (videoconferencia o vídeo-identificación) con seguridad equivalente a la presencia física.

RECUERDA

El período de vigencia de los certificados cualificados **no será superior a cinco años** (art. 4.2). Los certificados se extinguen por **caducidad** o por **revocación** (art. 5). La identificación del solicitante de un certificado cualificado exige, como regla, su **personación** (art. 7.1), salvo firma legitimada notarialmente o medios de identificación a distancia de seguridad equivalente.

5. El Documento Nacional de Identidad electrónico y sus certificados

El **DNI electrónico** es la principal manifestación práctica de un certificado cualificado en España. La Ley 6/2020 le dedica su **Disposición adicional tercera**, que lo define y equipara plenamente a los servicios de confianza cualificados:

Disposición adicional tercera · Documento Nacional de Identidad y sus certificados electrónicos

1. El **Documento Nacional de Identidad electrónico** es el Documento Nacional de Identidad que permite **acreditar electrónicamente la identidad personal** de su titular, en los términos establecidos en el artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, así como la **firma electrónica de documentos**.
2. Todas las personas físicas o jurídicas, públicas o privadas, **reconocerán la eficacia** del Documento Nacional de Identidad para acreditar la identidad y los demás datos personales del titular que consten en el mismo, así como

la identidad del firmante y la integridad de los documentos firmados con sus certificados electrónicos.

3. Los órganos competentes del **Ministerio del Interior** para la expedición del Documento Nacional de Identidad **cumplirán las obligaciones** que la presente Ley impone a los prestadores de servicios electrónicos de confianza que expidan **certificados cualificados**.
4. Sin perjuicio de la aplicación de la normativa vigente en materia del Documento Nacional de Identidad en todo aquello que se adecúe a sus características particulares, el Documento Nacional de Identidad se **regirá por su normativa específica**.

Hasta el desarrollo reglamentario del DNI previsto por la propia Ley, su **disposición transitoria segunda** mantiene en vigor el **Real Decreto 1553/2005, de 23 de diciembre**, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

6. Las obligaciones de los prestadores de servicios de confianza

El **Título III** de la Ley 6/2020 (arts. 8 a 13) impone a los prestadores una batería de obligaciones que el examen pregunta con frecuencia, sobre todo en torno al inicio de la actividad, el cese y la seguridad.

Artículo 12 · Inicio de la prestación de servicios electrónicos de confianza no cualificados

Los prestadores de servicios de confianza no cualificados **no necesitan verificación administrativa previa** de cumplimiento de requisitos para iniciar su actividad, pero deberán comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el **plazo de tres meses** desde que la inicien (...).

Artículo 9 · Obligaciones de los prestadores (extracto)

1. Los prestadores de servicios electrónicos de confianza deberán:
 - b) **No almacenar ni copiar**, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.
2. Los prestadores de servicios de confianza que expidan certificados electrónicos deberán disponer de un **servicio de consulta sobre el estado de validez o revocación** de los certificados emitidos accesible al público.
3. Los prestadores cualificados de servicios electrónicos de confianza deberán cumplir las siguientes obligaciones adicionales:
 - c) El prestador cualificado que vaya a cesar en su actividad deberá comunicarlo a los clientes a los que preste sus servicios y al órgano de supervisión con una **antelación mínima de dos meses** al cese efectivo de la actividad (...). En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier **proceso concursal** que se siga contra él.

Artículo 13.2 · Deber de resolver incidentes de seguridad

2. Los prestadores de servicios tienen la obligación de tomar las medidas necesarias para **resolver los incidentes de seguridad** que les afecten.

MATIZ

El **cese** del prestador no revoca el certificado «en todo caso». El art. 5.1.f) fija como causa de revocación el «**cese en la actividad del prestador de servicios de confianza salvo que la gestión de los certificados electrónicos expedidos por aquel sea transferida a otro prestador**»: si hay transferencia, el certificado no se revoca.

RECUERDA

Prestadores **no cualificados**: NO precisan verificación administrativa previa, pero comunican su actividad al Ministerio en **3 meses** (art. 12). Todo prestador debe **no almacenar ni copiar** los datos de creación de firma del cliente —salvo gestión en su nombre— y ofrecer un **servicio de consulta de validez/revocación** (art. 9). El prestador cualificado que **cesa** avisa con **2 meses** de antelación y comunica el **concurso** (art. 9.3.c); y todos deben **resolver los incidentes** de seguridad (art. 13.2).

TEMA 17

Epígrafe 3 — La ciberseguridad: principios y recomendaciones básicas

La ciberseguridad agrupa el conjunto de medidas técnicas, organizativas y de comportamiento dirigidas a proteger la información y los sistemas que la tratan frente a accesos no autorizados, alteraciones, pérdidas o usos ilícitos. En el ámbito público español, la referencia técnica en la respuesta a incidentes es el **CCN-CERT**, la **Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN)**, organismo adscrito al **Centro Nacional de Inteligencia (CNI)**. El CCN-CERT presta servicios de prevención, detección y respuesta ante ciberataques a las administraciones públicas y publica guías (serie **CCN-STIC**) e informes de **buenas prácticas** que sistematizan las recomendaciones básicas que se describen a continuación.

1. El CCN-CERT y el enfoque de las recomendaciones básicas

Las recomendaciones de ciberseguridad parten de una premisa: la mayor parte de los incidentes no explota fallos sofisticados, sino descuidos del usuario —contraseñas débiles, software sin actualizar, confianza en enlaces o adjuntos maliciosos—. Por eso el CCN-CERT organiza sus consejos por **factores de amenaza** (los escenarios de riesgo cotidianos) y por **medidas de protección** asociadas a cada uno. El objetivo común es reducir la **superficie de exposición**: mantener los sistemas actualizados, aplicar el **principio de mínima confianza** ante lo desconocido y verificar la identidad de quien envía información o solicita datos.

RECUERDA

El CCN-CERT es la **Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN)**, organismo adscrito al **Centro Nacional de Inteligencia (CNI)**. Actúa como CERT gubernamental de referencia para las administraciones públicas y difunde guías **CCN-STIC** e informes de buenas prácticas en materia de ciberseguridad.

Para ordenar esas amenazas por su gravedad, el CCN-CERT propone la «**Pirámide del Daño**», que jerarquiza las ciberamenazas **según su origen**, de mayor a menor peligrosidad:

Nivel	Origen de la amenaza	Peligrosidad
Vértice	Acciones patrocinadas por Estados (ciberspionaje, APT), industrias o empresas; dirigidas contra Administraciones, empresas de defensa, organizaciones de I+D e infraestructuras críticas	Máxima
Intermedio	Actores externos con ánimo de lucro económico (ciberdelincuencia)	Media
Base	Antiguos empleados , actores inexpertos y usuarios poco cuidadosos	Menor

El **ciberspionaje** —ciberataques «originados o patrocinados por Estados»— ocupa el vértice por su enorme dificultad de atribución, su carácter dirigido (Amenazas Persistentes Avanzadas) y el valor político, estratégico o económico de la información perseguida.

RECUERDA

La **Pirámide del Daño** del CCN-CERT clasifica las ciberamenazas **según su origen**: en el **vértice** (máxima peligrosidad), las acciones **patrocinadas por Estados** (ciberespionaje/APT); en el nivel intermedio, la ciberdelincuencia con **ánimo de lucro** y en la base, **antiguos empleados** y **usuarios poco cuidadosos**.

2. La Internet profunda: web superficial, *deep web* y *dark web*

Internet se estructura en capas según su accesibilidad. La **web superficial** (*surface web*) es la porción indexada por los buscadores convencionales (Google, Bing) y accesible mediante una búsqueda ordinaria; representa una fracción minoritaria del total. La **internet profunda** (*deep web*) comprende todo el contenido **no indexado** por los buscadores: correo web, banca en línea, intranets corporativas, bases de datos y documentos protegidos por autenticación. Es contenido de uso cotidiano y perfectamente legal.

Dentro de la internet profunda se sitúa la **web oscura** (*dark web*), una porción pequeña accesible únicamente mediante software específico de **anonimización**, principalmente la red **Tor** (*The Onion Router*, con dominios .onion) y otras como I2P o Freenet. Estas redes ocultan el origen y el destino de las comunicaciones. Junto a usos legítimos —protección de periodistas, denunciantes o disidentes en regímenes represivos—, la web oscura alberga **mercados ilícitos**: venta de drogas, armas, datos robados, credenciales y programas maliciosos.

MATIZ

La **internet profunda** (*deep web*) **NO** es sinónimo de **web oscura** (*dark web*). La *deep web* abarca todo el contenido no indexado por los buscadores —correo web, banca en línea, bases de datos, intranets—, de uso cotidiano y legal. La *dark web* es solo una porción reducida de aquella, accesible únicamente mediante redes de anonimización como Tor, donde conviven usos legítimos y mercados ilícitos.

Dos datos técnicos que el examen extrae de las guías del CCN-CERT cierran este apartado:

- **Origen de la red Tor.** «The Onion Router (TOR) fue un proyecto **diseñado e implementado por la Marina de los Estados Unidos**, lanzado en **2002**», con el fin de fortalecer las comunicaciones por Internet y garantizar el anonimato y la privacidad. Encamina el tráfico cifrado a través de **tres nodos** elegidos al azar (entrada, intermedio y salida), de modo que ningún nodo conoce a la vez el origen y el destino.
- **Bitcoin y la cadena de bloques.** El **bitcoin** es una moneda electrónica cifrada, **descentralizada** y de ordenador a ordenador (*peer-to-peer*), fuera del control de cualquier gobierno o entidad financiera; se intercambia mediante **billeteras digitales** (*wallets*). Cada transacción se registra en una gran base de datos, la **cadena de bloques** (*Blockchain*), en la que cada bloque nuevo contiene el *hash* del anterior y, con él, todo el historial. El CCN-CERT advierte de que representa «un mecanismo muy práctico para **blanquear dinero** y evadir impuestos».

RECUERDA

La red **Tor** (*The Onion Router*) fue **diseñada e implementada por la Marina de los Estados Unidos** (lanzada en **2002**) y encamina el tráfico por **tres nodos** cifrados. El **bitcoin** es una criptomoneda **descentralizada** *peer-to-peer* cuyas transacciones se anotan en la **blockchain** (cada bloque incorpora el *hash* del anterior); el CCN-CERT lo señala como vía habitual de **blanqueo** de capitales.

3. Navegación segura

El navegador es la principal vía de contacto con contenidos externos y, por ello, un objetivo frecuente. Las recomendaciones básicas persiguen que la comunicación sea confidencial y que el contenido cargado no comprometa el equipo:

- Navegar preferentemente por sitios que empleen el protocolo **HTTPS**, que cifra la comunicación mediante **TLS** y muestra el icono de candado; comprobar la validez del **certificado**.
- Mantener actualizados el **navegador** y sus **complementos** (*plugins*), e instalar únicamente extensiones de origen verificado y estrictamente necesarias.
- Verificar la **dirección (URL)** completa antes de introducir datos, para detectar dominios fraudulentos que imitan a los legítimos (*typosquatting*).

- Gestionar las **cookies** y borrar periódicamente los datos de navegación; recordar que el modo de navegación privada evita el rastro local, pero **no proporciona anonimato** frente a terceros.
- Desconfiar de **descargas** no solicitadas y de ventanas emergentes que ofrecen premios o alertan de supuestas infecciones.

MATIZ

El candado y el protocolo **HTTPS** solo garantizan que la comunicación con el sitio viaja **cifrada**, no que el sitio sea **legítimo** ni de confianza. Un portal fraudulento de *phishing* puede disponer de un certificado válido y mostrar el candado. La verificación exige comprobar además la **dirección exacta (URL)** y la identidad real del titular del sitio.

4. Seguridad del correo electrónico: el *phishing*

El correo electrónico es uno de los vectores de ataque más habituales. El *phishing* consiste en la **suplantación de la identidad** de una entidad de confianza —un banco, una administración pública, un proveedor de servicios— mediante mensajes que imitan su apariencia para engañar a la víctima y lograr que revele **credenciales** o datos, realice un pago o instale un programa malicioso. Existen variantes según su alcance y canal: el *spear phishing* (dirigido a una persona concreta), el *whaling* (dirigido a directivos), el *smishing* (por SMS) y el *vishing* (por llamada de voz).

Las señales de alarma típicas son el **remitente falseado**, el tono de **urgencia** o amenaza, los errores gramaticales, los enlaces que no coinciden con el destino real y los **adjuntos** inesperados. Las recomendaciones básicas son: no abrir adjuntos ni pulsar enlaces de mensajes no solicitados, no facilitar credenciales por correo (ninguna entidad legítima las pide así), verificar el remitente por un canal alternativo y emplear **firma y cifrado digital** en las comunicaciones sensibles.

5. Virtualización

La **virtualización** permite ejecutar un sistema operativo **invitado** dentro de otro **anfitrión** mediante una **máquina virtual**, creando un entorno **aislado** del equipo real. Aplicada

a la seguridad, ofrece un espacio controlado —**entorno aislado** o *sandbox*— en el que abrir archivos dudosos, analizar programas maliciosos o navegar por sitios de confianza incierta sin exponer el sistema principal. Si el contenido resulta dañino, el impacto queda confinado a la máquina virtual, que puede **restaurarse a un estado previo** (*snapshot*) o eliminarse por completo. Es, por tanto, una medida de **contención** y de análisis que limita la propagación de una posible infección.

6. Seguridad en dispositivos móviles y redes inalámbricas (wifi)

Los **dispositivos móviles** (teléfonos inteligentes y tabletas) concentran gran cantidad de información personal y credenciales, lo que los convierte en objetivo prioritario. Las recomendaciones básicas son: instalar aplicaciones solo desde las **tiendas oficiales**, revisar los **permisos** que solicita cada aplicación, mantener actualizados el **sistema operativo** y las aplicaciones, activar el **bloqueo de pantalla** y el **cifrado** del dispositivo, realizar **copias de seguridad** y habilitar las funciones de **localización** y **borrado remoto** para casos de pérdida o robo.

En cuanto a las **redes inalámbricas (wifi)**, en la red propia debe cambiarse la contraseña por defecto del router y emplear cifrado robusto (**WPA2** o, preferentemente, **WPA3**). Las **redes públicas y abiertas** son especialmente peligrosas, ya que no cifran el tráfico y facilitan su **interceptación** o la suplantación del punto de acceso.

MATIZ

Las **redes wifi públicas y abiertas** no cifran el tráfico entre el dispositivo y el punto de acceso, lo que permite interceptarlo o suplantar el propio punto de acceso (*rogue AP*). Conviene evitar en ellas operaciones sensibles —banca, credenciales— y, cuando sean imprescindibles, canalizar la conexión a través de una **red privada virtual (VPN)** que cifre el tráfico de extremo a extremo.

7. Mensajería instantánea y redes sociales

Las aplicaciones de **mensajería instantánea** y las **redes sociales** exponen tanto la información compartida como la propia identidad. La primera medida es configurar adecuadamente la **privacidad**, limitando quién puede ver el perfil, las publicaciones o el

estado de conexión, y valorar el uso de servicios con **cifrado de extremo a extremo**, que impide que un tercero lea el contenido de los mensajes.

Los riesgos característicos derivan del **exceso de exposición** (*oversharing*): publicar en exceso datos personales, rutinas o **geolocalización** facilita la **ingeniería social** y la suplantación de identidad. Estos canales son, además, vía habitual de difusión de **enlaces maliciosos** y bulos, y escenario de conductas como el *grooming* (acoso a menores con fines sexuales) o la **sextorsión**. Conviene desconfiar de solicitudes de contacto desconocidas, no aceptar archivos o enlaces no solicitados y verificar la identidad real del interlocutor.

8. El Internet de las cosas (IoT)

El **Internet de las cosas** (*Internet of Things*, IoT) designa la conexión a la red de **objetos cotidianos** dotados de sensores y capacidad de comunicación: cámaras, electrodomésticos, dispositivos de domótica, *wearables*, vehículos o sistemas industriales. Su proliferación **amplía enormemente la superficie de ataque**, porque cada dispositivo conectado es un punto de entrada potencial. Las debilidades más frecuentes son las **contraseñas por defecto** que no se modifican, la **ausencia de actualizaciones de firmware** y el uso de **protocolos de comunicación inseguros**. Un dispositivo IoT comprometido puede espiar al usuario, servir de puerta de acceso al resto de la red doméstica o integrarse, junto a miles de otros, en una **red de bots** (*botnet*) para lanzar ataques masivos de **denegación de servicio (DDoS)**. Las medidas básicas pasan por cambiar las credenciales de fábrica, actualizar el firmware y, cuando sea posible, **segmentar** estos equipos en una red separada.

RECUERDA

El **Internet de las cosas (IoT)** conecta a la red objetos cotidianos —cámaras, electrodomésticos, *wearables*, domótica— y **amplía la superficie de ataque**. Sus principales debilidades son las **contraseñas por defecto** y la **falta de actualización del firmware**, que permiten integrar los dispositivos en **botnets** para lanzar ataques masivos de denegación de servicio.

TEMA 17

Epígrafe 4 — El Esquema Nacional de Interoperabilidad

1. Objeto y ámbito de aplicación

El **Esquema Nacional de Interoperabilidad (ENI)** se aprueba mediante el **Real Decreto 4/2010, de 8 de enero**, en desarrollo del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. No es una norma técnica aislada, sino el **marco de criterios y recomendaciones** que las Administraciones públicas deben tener en cuenta para que sus sistemas puedan entenderse entre sí. Su artículo de cabecera fija el objeto y define las tres dimensiones que vertebran toda la materia — **organizativa, semántica y técnica**— y su finalidad última: evitar la discriminación al ciudadano por su elección tecnológica.

Artículo 1 · Objeto

1. El presente real decreto tiene por objeto regular el **Esquema Nacional de Interoperabilidad** establecido en el artículo 42 de la Ley 11/2007, de 22 de junio.
2. El Esquema Nacional de Interoperabilidad comprenderá los **criterios y recomendaciones** de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de **interoperabilidad organizativa, semántica y técnica** de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para **evitar la discriminación a los ciudadanos por razón de su elección tecnológica**.

El **ámbito de aplicación** no se define de forma autónoma: el ENI se remite al artículo 2 de la Ley 11/2007 (todas las Administraciones públicas y las relaciones de los ciudadanos con ellas por medios electrónicos). La nota clave del artículo 3 es la **regla de prevalencia**: el ENI y sus normas de desarrollo se imponen a cualquier otro criterio en materia de política de interoperabilidad.

Artículo 3 · Ámbito de aplicación

1. El ámbito de aplicación del presente real decreto será el establecido en el **artículo 2 de la Ley 11/2007, de 22 de junio**.
2. El Esquema Nacional de Interoperabilidad y sus normas de desarrollo, **prevalecerán sobre cualquier otro criterio** en materia de política de interoperabilidad en la utilización de medios electrónicos para el acceso de los ciudadanos a los servicios públicos.

MATIZ

La **Ley 11/2007, de 22 de junio**, de acceso electrónico de los ciudadanos a los servicios públicos —a la que el RD 4/2010 se remite— fue **derogada** por las Leyes 39/2015 (LPAC) y 40/2015 (LRJSP), con efectos de 2 de octubre de 2016. El **RD 4/2010 sigue vigente** y su articulado conserva la remisión formal al art. 42 de aquella (base legal histórica), pero el marco general del acceso electrónico está hoy en las Leyes 39/2015 y 40/2015; la cobertura legal vigente del ENI es el **art. 156 de la Ley 40/2015**.

MATIZ

No debe confundirse *interoperabilidad* con *seguridad*. El ENI (RD 4/2010) regula que los sistemas puedan comunicarse e intercambiar información con validez; el **Esquema Nacional de Seguridad (ENS)** regula la protección de esos sistemas. Son dos esquemas hermanos, nacidos en paralelo en 2010 con el mismo origen legal (art. 42 y disp. final 8.^a de la Ley 11/2007), pero con objeto distinto. El **Esquema Nacional de Seguridad vigente** es el **RD 311/2022, de 3 de mayo**, que derogó el RD 3/2010 y se ampara ya en el **art. 156.2 de la Ley 40/2015**.

2. Los principios básicos del Esquema Nacional de Interoperabilidad

El **artículo 4** es el precepto que enumera los principios. Opera en dos planos: remite a los **principios generales** del artículo 4 de la Ley 11/2007 (marco general del acceso electrónico) y añade **tres principios específicos** propios de la interoperabilidad, cada uno de los cuales se desarrolla después en su propio artículo (arts. 5, 6 y 7).

Artículo 4 · Principios básicos del Esquema Nacional de Interoperabilidad

La aplicación del Esquema Nacional de Interoperabilidad se desarrollará de acuerdo con los **principios generales** establecidos en el **artículo 4 de la Ley 11/2007**, de 22 de junio, y con los siguientes **principios específicos** de la interoperabilidad:

- a) La interoperabilidad como **cualidad integral**.
- b) **Carácter multidimensional** de la interoperabilidad.
- c) **Enfoque de soluciones multilaterales**.

Cada principio específico tiene un contenido preciso, resumido a partir de los artículos 5 a 7:

- **Cualidad integral (art. 5)** — la interoperabilidad se tiene presente de forma integral desde la concepción de los servicios y sistemas y a lo largo de todo su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión.
- **Carácter multidimensional (art. 6)** — la interoperabilidad se contempla en sus tres dimensiones (organizativa, semántica y técnica), más la dimensión temporal.
- **Enfoque de soluciones multilaterales (art. 7)** — se favorece la aproximación multilateral para aprovechar el escalado, las arquitecturas modulares y multiplataforma, y la lógica de compartir, reutilizar y colaborar.

RECUERDA

Principios específicos del ENI (art. 4): a) interoperabilidad como cualidad integral · b) carácter multidimensional · c) enfoque de soluciones multilaterales. Se suman a los principios generales del art. 4 de la Ley 11/2007. No confundir estos tres principios específicos con las tres dimensiones (organizativa, semántica y técnica), que son el contenido del segundo principio.

3. Las dimensiones de la interoperabilidad

El principio multidimensional del artículo 6 es el corazón del ENI. Su literal fija las tres dimensiones y advierte, además, de una cuarta perspectiva —la **dimensión temporal**— que garantiza el acceso a la información a lo largo del tiempo.

Artículo 6 · Carácter multidimensional de la interoperabilidad

La interoperabilidad se entenderá contemplando sus **dimensiones organizativa, semántica y técnica**. La cadena de interoperabilidad se manifiesta en la práctica en los **acuerdos interadministrativos**, en el **despliegue de los sistemas y servicios**, en la **determinación y uso de estándares**, en las **infraestructuras y servicios básicos** de las Administraciones públicas y en la **publicación y reutilización de las aplicaciones** de las Administraciones

públicas, de la documentación asociada y de otros objetos de información. Todo ello sin olvidar la **dimensión temporal** que ha de garantizar el acceso a la información a lo largo del tiempo.

Cada dimensión tiene su propio capítulo de desarrollo dentro del real decreto y una definición en el Glosario del anexo:

Dimensión	Capítulo	En qué consiste
Organizativa	Cap. III (arts. 8-9)	Capacidad de las entidades y de sus procesos para colaborar con el objeto de alcanzar logros mutuamente acordados sobre los servicios que prestan (servicios disponibles por medios electrónicos, inventarios de información administrativa).
Semántica	Cap. IV (art. 10)	Que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación (activos semánticos).
Técnica	Cap. V (art. 11)	Relación entre sistemas y servicios de tecnologías de la información: interfaces, interconexión, integración de datos y servicios, presentación, accesibilidad y seguridad (estándares abiertos aplicables).

MATIZ

Junto a las tres dimensiones clásicas, el ENI reconoce una **interoperabilidad en el tiempo**: la interacción entre elementos de distintas oleadas tecnológicas, que se manifiesta sobre todo en la **conservación de la información** en soporte electrónico. Por eso el ENI dedica un capítulo entero (Cap. X) a la recuperación y conservación del documento electrónico a largo plazo.

4. Las normas técnicas de interoperabilidad y su relación con el ENS

El real decreto contiene los criterios generales, pero su concreción operativa se remite a las **Normas Técnicas de Interoperabilidad (NTI)**. La **disposición adicional primera** ordena desarrollar un catálogo de NTI de **obligado cumplimiento** para todas las Administraciones públicas —documento electrónico, digitalización, expediente electrónico, política de firma, catálogo de estándares, modelos de datos, etc.—, elaboradas por los órganos competentes de la Administración General del Estado con participación de las demás Administraciones y publicadas mediante **Resolución** en el BOE. Son, por tanto, el nivel reglamentario de detalle que hace aplicable el ENI en la práctica.

En materia de **seguridad**, el ENI no duplica al ENS: se remite a él. El preámbulo lo declara expresamente —el ENI «se remite al Esquema Nacional de Seguridad para las cuestiones relativas en materia de seguridad que vayan más allá de los aspectos necesarios para garantizar la interoperabilidad»— y el artículo 22 lo articula para la conservación del documento electrónico.

Artículo 22 · Seguridad (apartado 1)

1. Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el **Esquema Nacional de Seguridad** en cuanto al cumplimiento de los **principios básicos** y de los **requisitos mínimos de seguridad** mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en los que se almacenen los documentos, de acuerdo con la **categorización de los sistemas**.

Los apartados siguientes del artículo 22 remiten la protección de los datos de carácter personal a su normativa propia (apdo. 2) y precisan que las medidas persiguen garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación de los documentos, atendiendo a los riesgos y a los plazos de conservación (apdo. 3).

RECUERDA

ENI ↔ ENS: mismo origen legal (art. 42 y disp. final 8.^a de la Ley 11/2007), objeto distinto y **relación de remisión**. El ENI garantiza que los sistemas se entiendan; para todo lo que exceda de lo necesario para la interoperabilidad, remite al ENS (principios básicos, requisitos mínimos y categorización de los sistemas). Las **Normas Técnicas de Interoperabilidad** (disp. adic. 1.^a) son su desarrollo obligatorio, aprobado por Resolución.

5. La reutilización y el licenciamiento de las aplicaciones

Entre los eslabones de la cadena de interoperabilidad está la **publicación y reutilización de las aplicaciones**. El **artículo 16** fija las condiciones de licenciamiento cuando una Administración pone su software a disposición de otra Administración o de la ciudadanía.

Artículo 16 · Condiciones de licenciamiento aplicables (apartado 1)

1. Las condiciones de licenciamiento de las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información cuya titularidad de los derechos de la propiedad intelectual sea de una Administración Pública (...) tendrán en cuenta los siguientes aspectos:
 - a) El fin perseguido es el **aprovechamiento y la reutilización de recursos públicos**.
 - b) La completa protección contra su **apropiación exclusiva o parcial** por parte de terceros.
 - c) La **exención de responsabilidad del cedente** por el posible mal uso por parte del cesionario.
 - d) La **no obligación de asistencia técnica o de mantenimiento** por parte del cedente.

- e) La **ausencia total de responsabilidad** por parte del cedente con respecto al cesionario en caso de errores o mal funcionamiento de la aplicación.
- f) El licenciamiento se realizará por defecto **sin contraprestación** y sin necesidad de establecer convenio alguno (...).

RECUERDA

Licenciamiento de aplicaciones públicas (art. 16 ENI): el fin es el **aprovechamiento y la reutilización** de recursos públicos; se protege contra la **apropiación exclusiva** el cedente queda **exento de responsabilidad** por el mal uso del cesionario y por errores o mal funcionamiento; **no** está obligado a asistencia técnica ni mantenimiento; y es **sin contraprestación** por defecto. Cuidado con el distractor: la responsabilidad NO recae en el cedente.

6. La conservación y recuperación del documento electrónico

El ENI persigue que el documento electrónico siga siendo accesible y fiable con el paso del tiempo (dimensión temporal). Tres preceptos concentran lo que el examen pregunta: las **medidas** de recuperación y conservación (art. 21), el **formato** de conservación (art. 23) y la **digitalización** del papel (art. 24).

Artículo 21 · Condiciones para la recuperación y conservación de documentos (extracto)

1. Las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:

- e) La **clasificación**, de acuerdo con un plan de clasificación adaptado a las funciones, tanto generales como específicas, de **cada una de las Administraciones públicas** (...).
- f) El **período de conservación** de los documentos, establecido por las **comisiones calificadoras** que correspondan (...).
- i) La **coordinación horizontal** entre el responsable de gestión de documentos y los restantes servicios interesados en materia de archivos.
- l) La **formación tecnológica** del personal responsable de la ejecución y del control de la gestión de documentos (...).

MATIZ

El plan de **clasificación** es **propio de cada Administración** («adaptado a las funciones... de cada una de las Administraciones públicas»), NO un «plan único de clasificación del conjunto de las AAPP». Y el **período de conservación** lo fijan las **comisiones calificadoras**, no libremente el órgano que custodia el documento.

Artículo 23 · Formatos de los documentos (apartado 1)

1. Con el fin de garantizar la conservación, el documento se conservará en el formato en que haya sido elaborado, enviado o recibido, y preferentemente en un formato correspondiente a un **estándar abierto** que preserve a lo largo del tiempo la **integridad del contenido** del documento, de la **firma electrónica** y de los **metadatos** que lo acompañan.

Artículo 24 · Digitalización de documentos en soporte papel

1. La digitalización de documentos en soporte papel por parte de las Administraciones públicas se realizará de acuerdo con lo indicado en la norma técnica de interoperabilidad correspondiente en relación con los siguientes aspectos:
 - a) Formatos estándares de uso común para la digitalización de documentos en soporte papel y técnica de compresión empleada (...).
 - b) Nivel de resolución.
 - c) Garantía de imagen fiel e íntegra.
 - d) Metadatos mínimos obligatorios y complementarios, asociados al proceso de digitalización.

RECUERDA

Conservación en el ENI: el formato preferente es un **estándar abierto** que preserve la integridad del **contenido, de la firma electrónica y de los metadatos** (art. 23.1 → la respuesta «todo lo anterior»). La **digitalización** del papel (art. 24) atiende a **formato/compresión, nivel de resolución, imagen fiel e íntegra y metadatos** —el «tamaño del documento» NO es uno de sus aspectos —.

TU OPOSICIÓN, EN UNA APP

El temario que tienes en las manos cobra vida en la app Persevera, con todo para estudiarlo:

tests · psicotécnicos · flashcards con repaso espaciado · supuestos
cursos · simulacros · mapas mentales · tutor IA · planificador

7 días de prueba · Suscripción sin permanencia: cancelas cuando quieras.

**APP STORE**

para iPhone y iPad

**GOOGLE PLAY**

para Android

**EN LA WEB**app.perseveraoposiciones.com

DEL MISMO EQUIPO



Eroodite — Estudia cualquier cosa con IA

Persevera es para tu oposición. **Eroodite, para todo lo demás:** tu carrera universitaria, otras oposiciones o cualquier material que caiga en tus manos. Sube tus apuntes, PDFs, vídeos de YouTube o fotos y su inteligencia artificial te crea al momento exámenes, fichas de repaso, resúmenes y mapas mentales. Con un tutor con IA que resuelve dudas —hasta las que le haces una foto—, repaso espaciado y modo concentración.

Tus apuntes, listos para estudiar en segundos. Empieza gratis.

**APP STORE**

para iPhone y iPad

**GOOGLE PLAY**

para Android