GUARDIA CIVIL

Tema 17

Resumen

# Materias Técnico-Científicas. Tecnologías de la Información y la Comunicación

**Opositu: prepara tu oposición con superpoderes.**

**Después de leerlo, ponte a prueba**

→ opositu.com/guardia-civil

Edición: Noviembre 2026

© 2026 Opositu. Todos los derechos reservados. · opositu.com

opositu

CÓMO ESTUDIAR

# Saca el máximo partido a este resumen

Estudiar no es solo leer y memorizar. Estos pasos te acercan a tu plaza.

1. **Lee el resumen entero.** Una primera pasada sin subrayar, solo para ver de qué va y cómo encaja todo.

2. **Relee fijándote en las partes subrayadas.** Fíjate en las trampas, los plazos y los artículos estrella: son los que más se repiten en el examen.

3. **Ponte a prueba.** Cierra el PDF e intenta recordarlo. Lo que recuerdes sin mirar es lo que de verdad sabes; si hay algo que te cuesta recordar, repásalo de nuevo.

4. **Utiliza repetición espaciada.** Vuelve al tema a los pocos días y otra vez en una semana. Repasar conceptos antes de olvidarlos ayuda a fijarlos en la memoria.

   • En Opositu, las fichas de estudio aplican la repetición espaciada por ti.

5. **Practica con preguntas tipo test.** En opositu.com cada pregunta de nuestro banco de preguntas propio de este tema incluye el razonamiento de por qué la respuesta correcta es correcta. Así aprendes de cada fallo.

6. **Haz simulacros de examen.** Cuando ya domines el tema, ponte a prueba en condiciones reales. Puedes hacerlo con un simulacro en PDF de convocatorias anteriores de los disponibles en internet o en opositu.com, con los razonamientos de exámenes pasados y tu nota calculada.


## Pon a prueba este tema en opositu.com

El examen es tipo test, así que prepararte con preguntas tipo test como las del examen es la mejor manera de practicar. En Opositu tienes preguntas de este mismo tema, simulacros con soluciones y razonamientos, y un porcentaje que estima tu nivel de preparación.

→ opositu.com/guardia-civil

ESCANEA Y EMPIEZA

ÍNDICE DEL RESUMEN

# Tema 17 · Materias Técnico-Científicas. Tecnologías de la Información y la Comunicación


01 Visión general del tema

02 Diagrama: vigencia, suspensión y extinción de un certificado (Ley 6/2020)

03 Esquema completo

04 Tablas comparativas

05 Plazos y cifras clave

06 Trampas frecuentes de examen

07 Reglas mnemotécnicas

08 Conexiones entre temas


opositu.com

# 01 Visión general del tema

Tema técnico-científico de las TIC: cubre la **Ley 11/2022 General de Telecomunicaciones** (objeto, principios, seguridad y secreto de las comunicaciones), el **RD 1125/2024** sobre gobernanza TIC en la Administración del Estado (que deroga el RD 806/2014), la **Ley 6/2020** sobre servicios electrónicos de confianza y firma electrónica, el **RD 4/2010 ENI**, la guía del CCN-CERT «Principios y recomendaciones básicas en Ciberseguridad» (resumen propio), la criptografía y un texto técnico sin fuente legal (electricidad y electromagnetismo, automovilismo, informática, ondas y telecomunicaciones), del que salieron todas las preguntas del tema de 2017 a 2019.

**Peso en examen**
Entre 2 y 5 preguntas por examen desde 2022 (2 en 2022-2A, 2023-1A y 2023-2A; 3 en 2022-1A, 2024-1A, 2024-2A, 2024-3A y 2025-A; 4 en 2026-A; 5 en 2022-Canarias-3A).

**Artículos estrella**
Ninguno: ningún artículo del tema se ha preguntado en tres convocatorias. En dos convocatorias: el art. 2 de la Ley 6/2020 (ámbito: 2022 y 2024), su art. 4 (vigencia: 2022 y 2026), su art. 5 (revocación y suspensión: 2021 y 2024) y el art. 3 del RD 1125/2024 (la CETIC: 2022 y 2024). También en dos convocatorias: la DA 1.ª del RD 4/2010 (2025 y 2026).

**Qué pesa más**
Las 34 preguntas del tema desde 2020, por norma: la **Ley 6/2020**, nueve (la revocación y la suspensión del art. 5, tres, dos de ellas con la trampa del cese «en todo caso»; la vigencia del art. 4 y el ámbito del art. 2, dos cada uno); el **RD 4/2010 ENI**, nueve (los principios del art. 4 y la DA 1.ª, dos cada uno); el **RD 1125/2024** (antes, el RD 806/2014), cinco (la CETIC, tres; las unidades TIC, dos), y la **Ley 11/2022**, cinco, una de ellas de 2020 sobre la Ley 9/2014 que la precedió.

Las otras seis son de la guía del **CCN-CERT** «Principios y recomendaciones básicas en Ciberseguridad», una pregunta en seis exámenes desde 2020 (**2020-2A, 2022-2A, 2024-1A, 2024-3A, 2025-A y 2026-A**): la red TOR, la Pirámide del Daño, bitcoin, el correo electrónico y la mensajería instantánea.

**Atención**
El RD 806/2014 fue derogado por el RD 1125/2024, de 5 de noviembre, en vigor desde el 7 de noviembre de 2024. Las preguntas anteriores a 2025 cuyo enunciado cita el RD 806/2014 deben releerse con el articulado nuevo: la sustancia (CETIC, medios transversales, antes «compartidos», proyectos de interés prioritario, unidades TIC) se mantiene; cambian los artículos y algunas denominaciones.

> **FUENTE** *Ley 11/2022 + RD 1125/2024 + Ley 6/2020 + RD 4/2010 ENI + guía del CCN-CERT*

## 02 Diagrama: vigencia, suspensión y extinción de un certificado (Ley 6/2020)

Cinco preguntas desde 2021 sobre un mismo asunto: la vida de un certificado electrónico según la **Ley 6/2020**. Un certificado se extingue por **caducidad**, al expirar su vigencia, o por **revocación** del prestador en los supuestos del art. 5.1 (**art. 4.1**). La vigencia de un certificado cualificado no será superior a **cinco años** (**art. 4.2**). La **suspensión** no lo extingue por sí sola: el prestador la acuerda en los supuestos a), c) y h) del art. 5.1, o si duda de los de b) y g), cuando sus prácticas de certificación la prevén (**art. 5.2**), y el certificado se extingue si vence el plazo de la suspensión sin que se haya levantado (**art. 5.3**). Ojo con el cese del prestador: revoca los certificados **salvo que su gestión pase a otro prestador** (art. 5.1.f), y dos exámenes pusieron la trampa del «en todo caso» (2021-1A y 2024-3A).

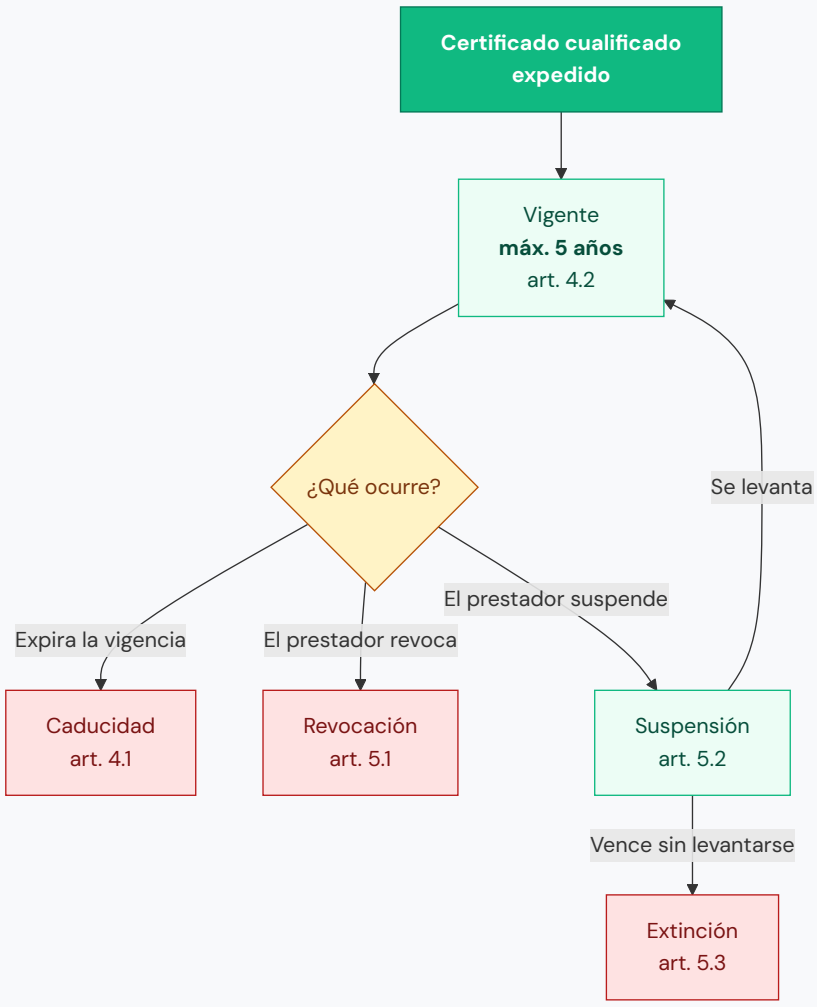



*Figura 1: Vigencia, suspensión y extinción de un certificado electrónico (arts. 4 y 5 Ley 6/2020)*

**FUENTE** *Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza*

## 03 Esquema completo

### 1. Ley 11/2022, de 28 de junio, General de Telecomunicaciones (Título I + Título III Cap. III)

- **Art. 1 Ley 11/2022 — Objeto y ámbito.** Regula las telecomunicaciones: 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 (art. 149.1.21.ª CE), y se aplica al dominio público radioeléctrico que usen todas las redes, públicas o no. **Quedan excluidos:** los servicios de comunicación audiovisual, los servicios de intercambio de vídeos a través de plataforma, los contenidos audiovisuales transmitidos a través de las redes y el régimen básico de los medios de comunicación social audiovisuales (art. 149.1.27.ª CE); y también los servicios que suministran contenidos transmitidos por las redes, el control editorial sobre ellos y los servicios de la sociedad de la información (Ley 34/2002), en tanto en cuanto no sean asimismo servicios de comunicaciones electrónicas.
- **Art. 2 Ley 11/2022 — Las telecomunicaciones como servicios de interés general.** Son **servicios de interés general que se prestan en régimen de libre competencia** (2.1). Solo tienen consideración de servicio público los del art. 4 (2.2; también art. 4.1).
- **Art. 3 Ley 11/2022 — Objetivos y principios.** Trece (letras a-m): a) fomentar la competencia efectiva y sostenible; b) desarrollar la economía y el empleo digital; c) promover el despliegue de redes y la prestación de servicios de comunicaciones electrónicas; d) impulsar la innovación en el despliegue de redes y la prestación de servicios; 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; g) promover la inversión eficiente en materia de infraestructuras; h) hacer posible el uso eficaz y eficiente de los recursos limitados, como la numeración y el espectro radioeléctrico; i) fomentar la **neutralidad tecnológica** en la regulación; j) garantizar el cumplimiento de las obligaciones de servicio público del título III, en especial las de servicio universal; k) defender los intereses de los usuarios; l) salvaguardar y proteger las necesidades de grupos sociales específicos, entre ellos las personas con discapacidad, las mayores y las que están en situación de dependencia; m) impulsar la universalización del acceso a las redes y servicios de comunicaciones electrónicas de banda ancha y contribuir a alcanzar la mayor vertebración territorial y social posible. (2023-1A, pregunta 86: la clave fue la e); las falsas deformaban la f, «mercado exterior e interior»; la i, «neutralidad ecológica», y la j, «servicio público y privado».)
- **Art. 4 Ley 11/2022 — Servicios para la seguridad nacional, defensa, seguridad pública, vial y protección civil.** Las redes y servicios para actividades esenciales de seguridad y defensa nacionales **se reservan al Estado** y se rigen por su normativa específica. Los bienes muebles o inmuebles vinculados a los centros, establecimientos y dependencias de las redes y de los servicios de comunicaciones electrónicas dispondrán de las medidas y sistemas de seguridad,

vigilancia, difusión de información, prevención de riesgos y protección que determine 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 (4.5; 2024-1A, pregunta 83). El Gobierno, con carácter excepcional y transitorio, puede acordar que la AGE asuma la gestión directa de determinados servicios de comunicaciones electrónicas disponibles al público, distintos de los servicios de comunicaciones interpersonales independientes de la numeración, o la explotación de ciertas redes públicas, para garantizar la seguridad pública y la seguridad nacional, sin que la intervención pueda vulnerar en ningún caso los derechos fundamentales; y también, previo informe preceptivo de la CNMC, ante el incumplimiento de las obligaciones de servicio público del título III. El acuerdo se comunica en **24 horas** al órgano jurisdiccional competente, que en **48 horas** establece si respeta los derechos fundamentales y libertades públicas y lo anula en caso negativo (4.6).

- **Art. 56 Ley 11/2022 — Salvaguardia de derechos fundamentales.** Las medidas sobre el acceso o el uso de servicios y aplicaciones por los usuarios finales respetarán los derechos y libertades fundamentales garantizados en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, la Carta de Derechos Fundamentales de la Unión Europea, los principios generales del Derecho comunitario y la Constitución Española (56.1; 2026-A, pregunta 80, dio como falsa la «Declaración de Libertades»). Una medida sobre el acceso o el uso de servicios y aplicaciones que pueda restringir esos derechos solo puede imponerse si es **adecuada, necesaria y proporcionada en una sociedad democrática** y su aplicación está sujeta a salvaguardias de procedimiento apropiadas: solo puede adoptarse respetando la presunción de inocencia, el derecho a la vida privada e intimidad, el derecho a la libertad de expresión e información y el derecho a la tutela judicial efectiva, mediante un procedimiento previo, justo e imparcial que incluya el derecho de los interesados a ser oídos, sin perjuicio de las condiciones procedimentales adecuadas en casos de urgencia debidamente justificados (56.2).
- **Art. 57 Ley 11/2022 — Principio de no discriminación.** Los operadores no aplicarán condiciones distintas por nacionalidad, residencia o lugar de establecimiento del usuario final, salvo que el trato diferente **se justifique de forma objetiva**.
- **Art. 58 Ley 11/2022 — Secreto de las comunicaciones.** Los operadores garantizan el secreto conforme a los **arts. 18.3 y 55.2 CE**. Los de redes públicas, servicios interpersonales basados en numeración o acceso a internet están obligados a realizar las interceptaciones que se autoricen judicialmente conforme al cap. V del título VIII del libro II de la LECrim, a la LO 2/2002 (control judicial previo del CNI) y a otras normas con rango de ley orgánica (58.2). Deben facilitar al agente facultado, de entre los siguientes, solo los datos indicados en la orden de interceptación legal y salvo que por las características del servicio no estén a su disposición (58.5 y 58.8): identidad del sujeto, identidad de las otras partes, servicios básicos y suplementarios, dirección de la comunicación, indicación de respuesta, causa de finalización, marcas temporales, información de localización y de señalización. Datos sobre la persona (58.6; también solo los que la orden indique): identificación, domicilio, número de titular, número de identificación del terminal, número de cuenta del proveedor, dirección de correo. Si aplican a las comunicaciones interceptadas compresión, cifrado, digitalización u otra

codificación, deben entregarlas **desprovistas de los efectos** de tales procedimientos, siempre que sean reversibles, con calidad no inferior a la del destinatario.

- **Art. 59 Ley 11/2022 — Interceptación por los servicios técnicos.** Para el control del dominio público radioeléctrico o localización de interferencias, la Administración reduce al mínimo el riesgo de afectar a los contenidos; si queda constancia de contenidos, sus soportes se custodian hasta que termine, en su caso, el expediente sancionador o, en otro caso, se destruyen inmediatamente, y nunca pueden divulgarse (59.1.b); las mismas reglas rigen la vigilancia del uso de las redes y de la prestación de los servicios (59.2).
- **Art. 60 Ley 11/2022 — Protección de datos de carácter personal.** Los operadores adoptan, como mínimo, estas medidas técnicas y de gestión: acceso a los datos solo del personal autorizado y para fines autorizados por la ley; protección de los datos frente a la destrucción accidental o ilícita, la pérdida o alteración accidentales y el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos; y una política de seguridad efectiva (60.1). Ante un **riesgo particular** de violación de la seguridad de la red o del servicio, el operador informa a los **abonados** del riesgo y de las medidas a adoptar (60.2; 2020-1A, pregunta 85, dio como falsa que informa a la AEPD). En caso de violación de datos personales, el operador notifica **sin dilaciones indebidas** a la **AEPD** y, si la violación puede afectar negativamente a la intimidad o a los datos personales de un abonado o particular, también a este; la notificación al abonado no es necesaria si el operador prueba a satisfacción de la AEPD que aplicó a los datos afectados medidas de protección tecnológica convenientes, como las que los hacen incomprensibles para quien no esté autorizado (60.3).



EJEMPLO PRÁCTICO — ART. 60.3 LEY 11/2022

### Filtración de datos personales de un operador

Javier abre el correo del lunes por la mañana y encuentra un mensaje de su compañía de telefonía móvil. Le informan de que, en un incidente de seguridad detectado el viernes anterior, su nombre, DNI y dirección postal podrían haber quedado expuestos a un acceso no autorizado. El operador le explica que ya ha notificado la incidencia **sin dilaciones indebidas** a la **Agencia Española de Protección de Datos** y le ofrece dos medidas para reducir el riesgo de suplantación de identidad.

*Cuando el examen pregunta por el art. 60 Ley 11/2022: **riesgo particular** de violación de la seguridad, a los **abonados** (60.2; 2020-1A dio como falsa la AEPD); **violación de datos personales**, a la **AEPD «sin dilaciones indebidas»** (60.3).*

**El art. 60.3 Ley 11/2022 obliga al operador a notificar *sin dilaciones indebidas* la violación de datos personales a la Agencia Española de Protección de Datos, y también al abonado o particular cuando la violación pueda afectar negativamente a su intimidad o a sus datos personales.**

- **Art. 61 Ley 11/2022 — Conservación y cesión de datos.** Se rige por la Ley 25/2007.

- **Art. 62 Ley 11/2022 — Cifrado.** Toda información que se transmita por las redes puede protegerse mediante cifrado (62.1). Cuando el cifrado se use para proteger la confidencialidad, puede imponerse la obligación de facilitar a un órgano de la AGE o a un organismo público los algoritmos o cualquier procedimiento de cifrado utilizado, en casos justificados de protección de los intereses esenciales de seguridad del Estado y la seguridad pública y para permitir la investigación, la detección y el enjuiciamiento de delitos, así como la de facilitar sin coste alguno los aparatos de cifra a efectos de su control (62.2). La información obtenida se trata con la máxima confidencialidad y se destruye una vez resuelta la amenaza o dictada sentencia firme sobre el delito (62.3).
- **Art. 63 Ley 11/2022 — Integridad y seguridad de redes y servicios.** Notificación al Ministerio competente de incidentes de seguridad con **impacto significativo**. Parámetros: número de usuarios afectados, duración, área geográfica, medida en que se ha visto afectado el funcionamiento, alcance económico y social. Cuando proceda, el Ministerio informa a las autoridades nacionales competentes de otros Estados miembros y a la **ENISA**; comunica a la Secretaría de Estado de Seguridad los incidentes que, afectando a operadores estratégicos nacionales, interesen a la protección de las infraestructuras críticas, y a la CNMC los que afecten o puedan afectar a las obligaciones específicas que ella haya impuesto.

## 2. RD 1125/2024, de 5 de noviembre — Organización TIC en la Administración del Estado (deroga el RD 806/2014)

- **Art. 1 RD 1125/2024 — Objeto.** Desarrollo de un **modelo común de gobernanza** de las TIC en la Administración General del Estado y sus organismos públicos y entidades de Derecho público vinculados o dependientes; incluye la **Estrategia TIC** y la mejora de los servicios públicos.
- **Art. 2 RD 1125/2024 — Ámbito.** **Administración del Estado**, entendida como AGE y sus organismos públicos y entidades de Derecho público vinculados o dependientes (Ley 40/2015). No alcanza a CCAA ni a EELL.
- **Art. 3 RD 1125/2024 — Comisión de Estrategia TIC (CETIC).** Órgano colegiado adscrito al **Ministerio para la Transformación Digital y de la Función Pública**. Composición (art. 3.2): preside la persona titular del Ministerio; **Vicepresidencia primera** = titular de la Secretaría de Estado de **Función Pública**; **Vicepresidencia segunda** = titular de la Secretaría de Estado de **Digitalización e Inteligencia Artificial**; vocales: titular de la Dirección de la Agencia Estatal de Administración Digital, un representante por cada ministerio (subsecretaría u órgano competente), titular de la D.G. de Gobernanza Pública, representante de la **Abogacía General del Estado, que actuará con voz pero sin voto**, y la persona titular de la Secretaría General de la Agencia como Secretario. Funciones (art. 3.3): fijar líneas estratégicas, aprobar la propuesta de Estrategia TIC para elevarla al Consejo de Ministros, informar anteproyectos de ley y reglamentos TIC, definir prioridades de inversión, declarar transversales determinados medios o servicios comunes y declarar proyectos de interés prioritario, ambos a propuesta del Consejo Rector de la Agencia (los proyectos, previo informe del ministerio con competencia en la materia), informar proyectos sectoriales e impulsar la colaboración con CCAA y EELL. Eleva anualmente al Consejo de Ministros un informe sobre la transformación digital. Se reúne **al**

**menos, trimestralmente** ; la convoca la presidencia, que puede invitar, con voz pero sin voto, a representantes de otros centros directivos e instituciones públicas.

- **Art. 7 RD 1125/2024 — Unidades TIC.** Son instrumentos fundamentales para la transformación digital de la Administración en los ámbitos sectoriales (7.1). Les corresponde la provisión sectorial de medios y servicios TIC **a sí mismas o a otras unidades administrativas**, con una o varias de estas 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) conformar la voluntad de adquisición de bienes o servicios TIC; i) las demás funciones relevantes en materia TIC (7.2). Se preguntaron en 2022 como art. 12 del RD 806/2014: «unidades administrativas», no «operativas» (2022-1A, pregunta 88), y consultoría «informática», no «telemática» (2022-Canarias-3A, pregunta 88).
- **Art. 8 RD 1125/2024 — Estrategia TIC.** El Gobierno, a iniciativa de la CETIC y propuesta del Ministerio, aprueba la **Estrategia TIC** ; determina objetivos, principios y acciones para el desarrollo de la administración digital.
- **Art. 9 RD 1125/2024 — Medios y servicios digitales comunes declarados transversales.** Se declaran transversales por la CETIC a propuesta del Consejo Rector de la Agencia cuando respondan a necesidades de un número significativo de unidades. Su uso es de **carácter obligatorio y sustitutivo** respecto a los medios particulares. La Agencia elabora el **Catálogo de Medios y Servicios Comunes**, que incluye todos los transversales.
- **Art. 10 RD 1125/2024 — Proyectos de interés prioritario.** Singular relevancia, especialmente los de colaboración con CCAA, EELL y UE; la declaración se traslada como recomendación **al Ministerio de Hacienda y a la Comisión de Políticas de Gasto** para que, en su caso, se tenga en cuenta en los PGE.

## 3. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

- **Art. 1 Ley 6/2020 — Objeto.** Complemento del **Reglamento (UE) 910/2014 (eIDAS)**.
- **Art. 2 Ley 6/2020 — Ámbito.** Se aplica a prestadores públicos y privados **establecidos en España** y a 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 Estado UE.
- **Art. 3 Ley 6/2020 — Efectos jurídicos de los documentos electrónicos.** Prueba: servicio no cualificado (art. 326.3 LEC); cualificado (art. 326.4 LEC).
- **Art. 4 Ley 6/2020 — Vigencia y caducidad.** Los certificados se extinguen por **caducidad** o **revocación**. El período de vigencia de los certificados cualificados **no será superior a cinco años** , fijado en atención a las características y tecnología empleada para generar los datos de creación de **firma, sello o autenticación de sitio web** (los tres: 2026-A, pregunta 81).

EJEMPLO PRÁCTICO — ART. 4.2 LEY 6/2020

### Un certificado digital caducado al firmar la renta



Carlos quiere firmar electrónicamente su declaración de la renta desde casa el último día del plazo. Al insertar el certificado digital en el navegador, la sede de la Agencia Tributaria le devuelve un error: el certificado ha expirado. Repasa los correos antiguos y comprueba que lo obtuvo en la FNMT hace casi seis años y que nunca lo renovó. No le va a quedar más remedio que solicitar uno nuevo y, mientras tanto, intentar firmar la declaración con Cl@ve PIN antes de que termine el plazo.

*En el art. 4.2 Ley 6/2020, la pista es **«no será superior a cinco años»**, según la tecnología de los datos de creación de firma, sello o autenticación de sitio web (2026-A); 2022-Canarias-3A dio seis meses, un año, tres años.*

**El art. 4.2 Ley 6/2020 establece que el período de vigencia de los certificados cualificados *no será superior a cinco años*, fijado en atención a las características y tecnología empleada para generar los datos de creación de firma, sello o autenticación de sitio web.**

- **Art. 5 Ley 6/2020 — Revocación y suspensión.** Supuestos de revocación (5.1): a) solicitud del firmante, la persona representada, un tercero autorizado, el creador del sello o el titular del certificado de autenticación de sitio web; b) violación o puesta en peligro del secreto de los datos de creación, o su utilización indebida por un tercero; c) resolución judicial o administrativa que lo ordene; d) fallecimiento o capacidad modificada judicialmente sobrevenida, total o parcial, del firmante, extinción de la personalidad jurídica o disolución del creador del sello en el caso de tratarse de una entidad sin personalidad jurídica, y cambio o pérdida de control sobre el nombre de dominio; e) terminación de la representación, cuya revocación deben pedir el representante y el representado; f) cese del prestador, salvo que la gestión de sus certificados se transfiera a otro prestador; g) falsedad o inexactitud de los datos aportados que constan en el certificado, o alteración posterior de las circunstancias verificadas; h) mecanismos criptográficos que no cumplen los estándares de seguridad mínimos; i) cualquier otra causa lícita prevista en la declaración de prácticas del servicio. Suspensión solo en a), c), h) y casos de duda en b) y g) si las prácticas lo prevén.



EJEMPLO PRÁCTICO — ART. 5.1 LEY 6/2020

### Solicitud urgente de revocación tras un robo

A Lucía le sustraen el bolso en una cafetería del centro de Valencia. Dentro estaba el móvil personal, donde tenía instalado su certificado digital de la FNMT y la aplicación de la Seguridad Social. Esa misma tarde, desde un teléfono prestado, llama al prestador de servicios de confianza para solicitar la revocación inmediata del certificado, antes de que quien tenga el móvil pueda usarlo para acceder a sus datos en la sede electrónica o suplantarla.

*Cuando el examen pregunta por el art. 5.1 Ley 6/2020, bastan la **solicitud del firmante** (a) o la **violación o puesta en peligro del secreto** (b), sin resolución (otro supuesto, c). Falsa en 2021-1A y 2024-3A: cese «en todo caso».*

**El art. 5.1 Ley 6/2020 obliga al prestador a revocar el certificado cuando lo solicita el firmante (letra a) o cuando se viola o se pone en peligro el secreto de los datos de creación de firma, o un tercero los utiliza indebidamente (letra b).**

- **Art. 6 Ley 6/2020 — Identidad del titular.** Persona física: nombre, apellidos y **DNI/NIE/NIF** (o pseudónimo inequívoco). Persona jurídica: denominación o razón social y NIF.
- **Art. 7 Ley 6/2020 — Comprobación de identidad.** Regla general: **personación** ante los encargados de verificarla; acreditación mediante DNI, pasaporte u otros medios admitidos en Derecho. Excepción: firma legitimada notarialmente, o identificación a distancia por videoconferencia o vídeo-identificación, en las condiciones que fije una Orden ministerial, con seguridad equivalente certificada por organismo de evaluación de la conformidad. Todo ello puede no exigirse si la identidad del solicitante ya constaba al prestador por una relación preexistente en la que se le identificó por personación (7.1) y el tiempo transcurrido desde esa identificación es **menor de cinco años** (7.6).

EJEMPLO PRÁCTICO — ART. 7.2 LEY 6/2020

### Obtener un certificado sin acudir a la oficina



Ana se ha mudado a un pueblo de la sierra de Soria y necesita un certificado cualificado para darse de alta como autónoma. La oficina de la FNMT más cercana está a setenta kilómetros. En la web del prestador descubre que puede identificarse mediante **vídeo-identificación**: una videollamada con un operador autorizado que verifica su DNI en cámara y graba la sesión. Veinte minutos después, Ana recibe el certificado emitido en su correo electrónico.

*En el art. 7.2 Ley 6/2020, lo decisivo es que la vídeo-identificación exige «una seguridad equivalente en términos de fiabilidad a la presencia física» certificada por un **organismo de evaluación de la conformidad**.*

**El art. 7.2 Ley 6/2020 admite, en las condiciones que fije una Orden ministerial, la identificación a distancia mediante videoconferencia o vídeo-identificación cuando aporte *seguridad equivalente en términos de fiabilidad a la presencia física* y dicha equivalencia esté certificada por un organismo de evaluación de la conformidad.**

- **Art. 8 Ley 6/2020 — Protección de datos personales.** Pseudónimos: el prestador conserva la documentación de la identidad real y la revela a órganos judiciales y autoridades públicas legalmente habilitadas.
- **Art. 9 Ley 6/2020 — Obligaciones de los prestadores.** Generales: publicar información veraz; **No almacenar ni copiar**, por sí o tercero, los datos de creación de firma, sello o

autenticación, salvo gestión en nombre del titular (con sistemas y productos fiables); y, si expiden certificados, disponer de un servicio de consulta accesible al público sobre el estado de validez o revocación (9.2). Adicionales para prestadores cualificados (art. 9.3): a) conservar información durante **15 años** **desde la extinción del certificado o la finalización del servicio prestado**; b) seguro de responsabilidad civil mínimo **1.500.000 euros** (excepto sector público), más **500.000 euros** por cada tipo de servicio cualificado adicional; c) comunicar el cese de actividad a clientes y al órgano de supervisión con una **antelación mínima de dos meses**, por un medio que acredite la entrega y recepción efectiva siempre que sea factible, y comunicar al órgano de supervisión cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad, en especial, en cuanto lo conozca, la apertura de cualquier proceso concursal que se siga contra él (2024-2A, pregunta 84); d) remitir el informe de evaluación de la conformidad al Ministerio en los términos del art. 20.1 del Reglamento (UE) 910/2014.

- **Art. 10 Ley 6/2020 — Responsabilidad de los prestadores.** Asumen **toda la responsabilidad frente a terceros** por la actuación de personas u otros prestadores en los que deleguen, incluida la comprobación de identidad previa a la expedición.
- **Art. 11 Ley 6/2020 — Limitaciones de responsabilidad.** El prestador no responde de los daños causados a la persona a la que presta el servicio o a terceros de buena fe si esa persona incurre en los supuestos del Reglamento (UE) 910/2014 o en estos: a) no le dio información veraz, completa y exacta, cuando el prestador, actuando con la debida diligencia, no pudo detectar la inexactitud; b) no le comunicó sin demora indebida cualquier modificación de las circunstancias que incidan en el servicio; c) fue negligente en la conservación de sus datos de creación de firma, sello o autenticación de sitio web, en el aseguramiento de su confidencialidad o en su protección frente a todo acceso o revelación o, en su caso, de los medios que den acceso a ellos; d) no pidió la suspensión o revocación del certificado en caso de duda sobre la confidencialidad de esos datos o, en su caso, de los medios que den acceso a ellos; e) usó esos datos expirado el período de validez del certificado o notificada por el prestador su extinción o suspensión (11.1). Tampoco responde si el **destinatario** actúa de forma negligente: no tiene en cuenta la suspensión o pérdida de vigencia del certificado, o no verifica la firma o el sello (11.2); ni de la inexactitud de los datos acreditados mediante documento público u oficial, inscrito en un registro público si así resulta exigible (11.3).
- **Art. 12 Ley 6/2020 — Inicio de prestación de servicios no cualificados.** **No necesitan verificación administrativa previa**; basta comunicar la actividad al Ministerio en el plazo de **tres meses** desde el inicio. El Ministerio publica en su web el listado de prestadores no cualificados (lista separada de la cualificada). En el mismo plazo deben comunicar la modificación de los datos inicialmente transmitidos y el cese de su actividad (2025-A, pregunta 83).
- **Art. 13 Ley 6/2020 — Obligaciones de seguridad.** Cualificados y no cualificados notifican al Ministerio las violaciones de seguridad o pérdidas de integridad del art. 19.2 del Reglamento (UE) 910/2014, sin perjuicio de notificarlas a la AEPD, a otros organismos relevantes o a las personas afectadas (13.1); deben tomar las medidas necesarias para resolver los incidentes de seguridad que les afecten (13.2; 2025-A, pregunta 83), y amplían la información de la

notificación inicial en un plazo máximo de **un mes** tras la notificación del incidente y, en su caso, tras su resolución (13.3).

- **DA 3.ª Ley 6/2020 — DNI electrónico.** Acredita electrónicamente la identidad personal (art. 8 LO 4/2015 Seguridad Ciudadana) y permite la firma electrónica. Lo expide el Ministerio del Interior, cuyos órganos competentes asumen las obligaciones de prestador cualificado.

## 4. RD 4/2010 ENI — Esquema Nacional de Interoperabilidad (de 8 de enero)

- **Art. 1 RD 4/2010 — Objeto.** Regula el ENI establecido en el **art. 42 de la Ley 11/2007** (hoy referido a Ley 40/2015). Comprende criterios y recomendaciones de seguridad, normalización y conservación para garantizar la interoperabilidad organizativa, semántica y técnica.
- **Art. 2 RD 4/2010 — Definiciones.** Remite al **Glosario de Términos incluido en el anexo**.
- **Art. 3 RD 4/2010 — Ámbito.** El del art. 2 de la Ley 11/2007. El ENI y sus normas de desarrollo **prevalecerán sobre cualquier otro criterio** en materia de política de interoperabilidad.
- **Art. 4 RD 4/2010 — Principios específicos.** Tres: a) **interoperabilidad como cualidad integral**; b) **carácter multidimensional de la interoperabilidad**; c) **enfoque de soluciones multilaterales**. (2022-1A preguntó cuál NO es principio; la respuesta era «la interoperabilidad como mecanismo de control».)
- **Art. 5 RD 4/2010 — Cualidad integral.** La interoperabilidad se tiene en cuenta desde la concepción y a lo largo de todo el **ciclo de vida** (planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión).
- **Art. 6 RD 4/2010 — Carácter multidimensional.** Dimensiones **organizativa, semántica y técnica**, más la dimensión temporal de conservación.
- **Art. 7 RD 4/2010 — Enfoque multilateral.** Aproximación multilateral para obtener ventajas del escalado, arquitecturas modulares y multiplataforma, compartir, reutilizar y colaborar.
- **Arts. 8-9 RD 4/2010 — Interoperabilidad organizativa.** Servicios disponibles por medios electrónicos: condiciones publicadas; uso de la **Red de comunicaciones de las AAPP españolas**; posibilidad de **nodos de interoperabilidad**. Inventarios de información administrativa: procedimientos (conectados al SIA del MPTFP) y órganos/oficinas (conectados al **Directorio Común de Unidades Orgánicas y Oficinas**).
- **Art. 10 RD 4/2010 — Interoperabilidad semántica.** La Relación de modelos de datos de intercambio comunes es de **preferente** aplicación (10.1); los modelos que establecen y publican los órganos con competencias en cada materia de intercambio son de **obligatoria** aplicación (10.2); unos y otros se publican a través del **Centro de Interoperabilidad Semántica de la Administración (CISE)** (10.3).
- **Art. 11 RD 4/2010 — Estándares aplicables.** Se usarán **estándares abiertos** y, en su caso y de forma complementaria, estándares de **uso generalizado por los ciudadanos**. En las relaciones con los ciudadanos y con otras Administraciones, el uso en exclusiva de un estándar no abierto sin alternativa abierta se limita a los casos en que no se disponga de un estándar abierto que satisfaga esa funcionalidad, y solo mientras no se disponga de él (11.2).

Criterios de selección: especificaciones técnicas TIC (Reglamento UE 1025/2012), definición de estándar abierto del anexo de la Ley 11/2007, carácter de especificación formalizada, coste que no suponga dificultad de acceso, adecuación a las necesidades, madurez y reutilización.

- **Art. 12 RD 4/2010 — Infraestructuras y servicios comunes.** Las AAPP **enlazarán** sus infraestructuras propias con las comunes que proporcione la AGE.
- **Art. 13 RD 4/2010 — Red de comunicaciones.** Para satisfacer el art. 43 Ley 11/2007, las AAPP utilizan preferentemente la **Red de comunicaciones de las AAPP españolas**, que es prestada por la **Red SARA** (no la Red Iris).
- **Art. 14 RD 4/2010 — Plan de direccionamiento.** Las AAPP aplican el Plan de direccionamiento e interconexión de redes desarrollado en la norma técnica correspondiente.
- **Art. 15 RD 4/2010 — Hora oficial.** Los sistemas se sincronizan con la hora oficial con precisión que garantice **la certidumbre de los plazos**. La sincronización se realiza con el **Real Instituto y Observatorio de la Armada** (RD 1308/1992) y, cuando sea posible, con la hora oficial europea.
- **Art. 16 RD 4/2010 — Condiciones de licenciamiento aplicables.** Las aplicaciones públicas se licencian con: a) fin de aprovechamiento y reutilización de recursos públicos; b) protección completa contra apropiación exclusiva; c) **exención de responsabilidad del cedente** por mal uso del cesionario; d) **no obligación de asistencia técnica o de mantenimiento** por parte del cedente; e) ausencia total de responsabilidad por errores; f) licenciamiento por defecto sin contraprestación. Para fuentes abiertas: ejecución para cualquier propósito, conocimiento del código, modificación y redistribución. Aplicación preferente: **Licencia Pública de la Unión Europea (EUPL)**.
- **Art. 17 RD 4/2010 — Directorios de aplicaciones reutilizables.** La AGE mantiene el Directorio general a través del **Centro de Transferencia de Tecnología** (art. 158 Ley 40/2015).
- **Art. 18 RD 4/2010 — Política de firma electrónica y certificados.** La AGE define la política marco; los organismos AGE la aplican; la no aplicación la justifica el órgano u organismo competente y la autoriza la SGAD (Secretaría General de Administración Digital).
- **Art. 20 RD 4/2010 — Plataformas de validación.** Proporcionan servicios de confianza en un único punto de llamada para integrar certificados y firmas de distintas AAPP, e incorporan las **listas de confianza** nacionales y europeas.
- **Art. 21 RD 4/2010 — Recuperación y conservación de documentos.** Medidas (21.1, letras a-m): a) política de gestión de documentos; b) **índice electrónico** firmado por el órgano actuante que garantice la integridad del expediente y permita su recuperación; c) identificación única e inequívoca de cada documento; d) **metadatos mínimos obligatorios** y, en su caso, complementarios; e) clasificación según un plan adaptado a las funciones, tanto generales como específicas, de cada una de las Administraciones públicas y de sus entidades de Derecho público vinculadas o dependientes (no un «plan único» común: 2023-2A, pregunta 87); f) período de conservación establecido por las comisiones calificadoras que correspondan; g) acceso completo e inmediato a los documentos; h) conservación a lo largo del ciclo de vida, según el art. 22; i) coordinación horizontal entre el responsable de gestión de

documentos y los demás servicios interesados en materia de archivos; j) transferencia, en su caso, de los expedientes entre repositorios electrónicos; k) borrado de la información o destrucción de los soportes si lo establece la evaluación documental, dejando registro; l) formación tecnológica del personal responsable; m) documentación de los procedimientos que garanticen la interoperabilidad a medio y largo plazo.

- **Art. 22 RD 4/2010 — Seguridad.** Para asegurar la conservación de los documentos electrónicos se aplica lo previsto en el Esquema Nacional de Seguridad (principios básicos y requisitos mínimos, con medidas adecuadas a los medios y soportes según la categorización de los sistemas) (22.1), con el fin de garantizar su integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica (22.3).
- **Art. 23 RD 4/2010 — Formatos.** El documento se conserva en el formato en que se elaboró/recibió y, preferentemente, en un **estándar abierto que preserve a lo largo del tiempo** la integridad del contenido, la firma y los metadatos. Si hay riesgo de obsolescencia: copiado auténtico con cambio de formato.
- **Art. 24 RD 4/2010 — Digitalización de documentos en soporte papel.** Conforme a la norma técnica: formatos estándares de uso común, técnica de compresión, nivel de resolución, garantía de imagen **fiel e íntegra**, metadatos mínimos obligatorios y complementarios.



EJEMPLO PRÁCTICO — ART. 24.1 RD 4/2010

### Digitalizar un documento en papel en el registro

Mateo se acerca a la oficina de registro de su ayuntamiento para presentar un certificado de nacimiento en papel exigido para una beca. La funcionaria recoge el documento, lo coloca en el escáner del mostrador, ajusta el nivel de resolución y comprueba en pantalla que la imagen resultante es **fiel e íntegra**. Después le entrega el resguardo y el documento original; el archivo digitalizado, con sus metadatos asociados, ya viaja por la red administrativa hacia el organismo destinatario.

*Cuando el examen pregunta por art. 24.1 RD 4/2010, 2022-Canarias-3A añadió uno que no está, el tamaño del documento; los cuatro son **formato y compresión, nivel de resolución, imagen fiel e íntegra y metadatos mínimos obligatorios y complementarios**.*

**El art. 24.1 RD 4/2010 exige que la digitalización de documentos en papel respete formatos estándares y técnica de compresión, nivel de resolución, *garantía de imagen fiel e íntegra* y metadatos mínimos obligatorios y complementarios asociados al proceso.**

- **Art. 25 RD 4/2010 — Sedes y registros electrónicos.** Su interoperabilidad y la del acceso electrónico de los ciudadanos se rige por el ENI.

EJEMPLO PRÁCTICO — ART. 25 RD 4/2010

### Tramitar el empadronamiento desde la sede del ayuntamiento



María acaba de mudarse a Sevilla con su pareja y necesita empadronarse en su nuevo domicilio. En vez de pedir cita presencial en el padrón, abre el navegador, accede a la **sede electrónica** del ayuntamiento, se identifica con su certificado digital y completa el trámite desde el sofá. Esa misma tarde recibe el justificante de empadronamiento en formato electrónico, con código seguro de verificación, en su carpeta ciudadana.

*Cuando el examen pregunta por art. 25 RD 4/2010, la **interoperabilidad** de sedes y registros electrónicos se rige por el **ENI**; 2024-2A puso en su lugar el ENS, el Sistema de Información Administrativa y el Comité Sectorial.*

**El art. 25 RD 4/2010 establece que la interoperabilidad de las sedes y registros electrónicos, así como del acceso electrónico de los ciudadanos a los servicios públicos, *se regirán por lo establecido en el Esquema Nacional de Interoperabilidad*.**

- **Arts. 26-28 RD 4/2010 — Normas de conformidad.** Inclusión en el ciclo de vida de servicios y sistemas; mecanismos de control en cada órgano; publicidad de las declaraciones de conformidad en las sedes electrónicas.
- **Art. 29 RD 4/2010 — Actualización permanente.** El ENI se desarrolla y perfecciona en paralelo al progreso de los servicios de Administración Electrónica.
- **DA 1.ª RD 4/2010 — Desarrollo del ENI.** Normas técnicas de interoperabilidad obligatorias (Catálogo de estándares, Documento electrónico, Digitalización, Expediente electrónico, Política de firma, Protocolos de intermediación, Modelos de datos, Política de gestión de documentos, Requisitos de conexión, Procedimientos de copiado auténtico, Modelo de Datos para intercambio de asientos, Reutilización de recursos…); las aprueba el **Ministerio para la Transformación Digital y de la Función Pública**, a propuesta de la Comisión Sectorial de Administración Electrónica, y se publican por Resolución de la persona titular de la Secretaría de Estado de Función Pública (DA 1.ª.2; 2026-A, pregunta 83). Para garantizar la debida interoperabilidad en materia de **ciberseguridad y criptografía** en la aplicación del ENI, el órgano competente es el **Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia**.

## 5. Ciberseguridad, criptografía y CCN-CERT (sin fuente legal directa)

- **Centro Criptológico Nacional (CCN).** Adscrito al Centro Nacional de Inteligencia, es el órgano competente para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía en la aplicación del ENI (DA 1.ª.3 RD 4/2010). Su capacidad de respuesta a incidentes es el **CCN-CERT**. La guía cita su plataforma multiantivirus **MARIA**, que analiza código dañino con varios motores.

- **CCN-CERT.** Capacidad de respuesta a incidentes de seguridad de la información del CCN, creada en 2006 como CERT gubernamental o nacional (guía BP/01, pág. 4). Le corresponden los ciberincidentes del **Sector Público**, los de las **empresas y organizaciones de interés estratégico** y los de cualquier **sistema clasificado**: la guía no lo limita a las Administraciones.
- **Criptografía simétrica.** Una sola clave secreta compartida entre emisor y receptor (AES, DES, 3DES). Rápida, ideal para grandes volúmenes; problema: distribución segura de la clave.
- **Criptografía asimétrica.** Par de claves: **pública** (cifrar o verificar) y **privada** (descifrar o firmar). Algoritmos: RSA, ECC, ElGamal. Soporta firma electrónica: el firmante firma con su clave privada; el receptor verifica con la clave pública.
- **Funciones hash criptográficas (SHA-256, SHA-3).** Generan una huella de longitud fija a partir de cualquier entrada. Propiedades: **unidireccionalidad** (no se puede invertir), **resistencia a colisiones**, determinismo.
- **Pirámide del Daño (guía BP/01, pág. 7).** Ordena las ciberamenazas en tres niveles de peligrosidad según su origen: en el más alto, las **acciones patrocinadas por Estados**; en el intermedio, los actores externos con ánimo de lucro económico; en el más bajo, los exempleados, los actores poco expertos y los usuarios poco cuidadosos. Visto en el examen 2024-3A.
- **Red TOR (guía BP/01, pág. 11).** The Onion Router es un proyecto que diseñó e implementó la **Marina de los Estados Unidos** y que se lanzó en **2002**, para reforzar la comunicación por Internet y asegurar el anonimato y la privacidad de quien la usa. Visto en el examen 2024-1A.

## 6. MATERIAS TÉCNICO-CIENTÍFICAS (sin fuente legal)

- **Magnitudes eléctricas.** Carga (culombio, C), intensidad (amperio, A; $I = Q/t$; 1 A = 1 C/s), tensión (voltio, V; 1 V = 1 J/C), resistencia (ohmio, Ω; 1 Ω = 1 V/A) y potencia (vatio, W; 1 W = 1 J/s); de ellas, solo el amperio es unidad básica del SI. El amperímetro se conecta en serie y el voltímetro en paralelo.
- **Ley de Ohm, potencia y energía.** $V = I \cdot R$; $P = V \cdot I = I^2 \cdot R = V^2/R$; $E = P \cdot t$ (1 kWh = $3{,}6 \times 10^6$ J).
- **Resistencia de un conductor.** $R = \rho \cdot L / S$: crece con la resistividad y la longitud, disminuye con la sección y, en los metales, aumenta con la temperatura. Mejores conductores: plata, cobre y aluminio.
- **Serie y paralelo.** Serie: misma intensidad, $R_eq = R_1 + R_2 + \ldots$ (mayor que la mayor). Paralelo: misma tensión, $1/R_eq = 1/R_1 + 1/R_2 + \ldots$ (menor que la menor); para dos, $R_1 \cdot R_2 / (R_1 + R_2)$.
- **Ley de Joule.** $Q = I^2 \cdot R \cdot t$, en julios; en calorías, $Q = 0{,}24 \cdot I^2 \cdot R \cdot t$. Es la base del fusible.
- **Magnetismo e inducción.** Los polos de un imán son inseparables; magnetismo remanente es el que conserva el material retirado el campo. La inducción magnética B se mide en teslas (1 T = 10.000 gauss) y el flujo en weber. Oersted (1820): toda corriente crea un campo magnético. Faraday: la variación del flujo induce una fem; Lenz: la corriente inducida se opone a la variación que la produce.

- **Ondas y espectro.** v = λ · f y T = 1/f. De menor a mayor frecuencia y energía: radio, microondas, infrarrojo, visible, ultravioleta, rayos X y gamma; la energía de cada fotón es E = h · f. El sonido es una onda mecánica y longitudinal, que no se propaga en el vacío.
- **Radiocomunicación.** El espectro radioeléctrico (frecuencias por debajo de 3.000 GHz, Ley 11/2022, anexo II; bandas habituales de 3 kHz a 300 GHz) lo gestiona la UIT: AM de onda media en MF, onda corta en HF, FM (87,5-108 MHz) en VHF, y TDT, telefonía móvil y GPS en UHF. La AM varía la amplitud de la portadora y la FM su frecuencia. Elementos de la comunicación: emisor, receptor, mensaje, canal, código y ruido.
- **Motor de cuatro tiempos.** Admisión, compresión, explosión o expansión (el único tiempo motriz) y escape, en dos vueltas del cigüeñal (720°); carrera es el recorrido del pistón entre el PMS y el PMI. En el diésel entra solo aire y el gasóleo se autoinflama por compresión, sin bujía de encendido.
- **Combustibles.** El octanaje mide la resistencia de la gasolina a detonar; el número de cetano, la facilidad del gasóleo para autoinflamarse (más cetano, menor retraso de la ignición).
- **Transmisión, refrigeración, frenos y dirección.** Transmisión: embrague, caja de cambios, árbol de transmisión, grupo cónico-diferencial y palieres; el árbol de levas es de la distribución. El termostato abre en torno a 85-90 °C. El ABS evita que las ruedas se bloqueen y conserva la dirección. Cotas de la dirección: avance, salida, caída y convergencia.
- **Informática.** Hardware y software; CPU: unidad de control, unidad aritmético-lógica y registros. RAM volátil y de lectura y escritura; ROM no volátil. 1 byte = 8 bits; 1 KB = 1.024 bytes; 1 TB = 1.024 GB. Disco duro: platos de dos caras, cada una con su cabezal; pistas concéntricas, que se dividen en sectores, la unidad mínima de lectura y escritura; y cilindros, las pistas alineadas de todos los platos. Generaciones: válvulas de vacío, transistores, circuitos integrados (el «chip»), microprocesadores y la quinta, en curso, asociada a la inteligencia artificial.

**FUENTE** *Arts. 1-4, 56-63 Ley 11/2022; arts. 1-3, 7-10 RD 1125/2024; arts. 1-13, DA 3.ª Ley 6/2020; arts. 1-29, DA 1.ª RD 4/2010; guía CCN-CERT; materias técnico-científicas (sin fuente legal)*

## 04 Tablas comparativas

### Tabla 1 — Servicios electrónicos de confianza: cualificados vs no cualificados (Ley 6/2020).

| ASPECTO | NO CUALIFICADOS | CUALIFICADOS |
|---|---|---|
| Inicio de actividad | Sin verificación administrativa previa (art. 12) | Verificación previa, evaluación de conformidad (art. 21 Reglamento UE 910/2014) |
| Comunicación al Ministerio | 3 meses desde el inicio (art. 12) | Antes del inicio |
| Lista publicada | Lista separada de no cualificados | Lista de confianza (TSL) |
| Plazo conservación información | No fijado en ley | 15 años desde extinción/finalización (art. 9.3.a) |
| Seguro responsabilidad civil | No exigido | Mínimo 1.500.000 € (+ 500.000 € por servicio adicional), salvo prestadores del sector público (art. 9.3.b) |
| Aviso de cese | Comunicación al Ministerio en 3 meses (art. 12) | 2 meses de antelación a clientes y Ministerio (art. 9.3.c) |

### Tabla 2 — Criptografía: simétrica vs asimétrica vs hash.

| TIPO | CLAVES | USO TÍPICO | ALGORITMOS |
|---|---|---|---|
| **Simétrica** | Una clave compartida | Cifrado de grandes volúmenes | AES, DES, 3DES, RC4 |
| **Asimétrica** | Par de claves (pública + privada) | Firma electrónica; intercambio seguro de clave | RSA, ECC, ElGamal, DSA |
| **Hash** | Ninguna (función unidireccional) | Integridad; huella digital del documento | SHA-256, SHA-3, MD5 (obsoleto) |

## Tabla 3 — Composición de la CETIC (RD 1125/2024 art. 3.2).

| CARGO | TITULAR |
|---|---|
| Presidencia | Titular del Ministerio para la Transformación Digital y de la Función Pública |
| Vicepresidencia primera | Titular de la Secretaría de Estado de Función Pública |
| Vicepresidencia segunda | Titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial |
| Vocales | Titular Dirección Agencia Estatal de Administración Digital; un representante por ministerio (Subsecretaría); titular D.G. Gobernanza Pública; representante Abogacía General del Estado (con voz, sin voto) |
| Secretaría | Titular de la Secretaría General de la Agencia |
| Periodicidad | Al menos, trimestralmente |

**FUENTE** *arts. 9, 12 Ley 6/2020; art. 3.2 RD 1125/2024*

## 05 Plazos y cifras clave

| CONCEPTO | PLAZO / CIFRA | ARTÍCULO |
|---|---|---|
| Vigencia máxima de los certificados cualificados | 5 años | Art. 4.2 Ley 6/2020 |
| Conservación de información del servicio cualificado | 15 años desde extinción o finalización | Art. 9.3.a Ley 6/2020 |
| Seguro mínimo de responsabilidad civil (prestador cualificado, salvo sector público) | 1.500.000 € | Art. 9.3.b Ley 6/2020 |
| Suplemento por cada servicio cualificado adicional | 500.000 € | Art. 9.3.b Ley 6/2020 |
| Antelación para comunicar cese de actividad | 2 meses antes del cese efectivo | Art. 9.3.c Ley 6/2020 |
| Plazo para comunicar inicio actividad (no cualificados) | 3 meses desde el inicio | Art. 12 Ley 6/2020 |
| Plazo para ampliar información tras incidente | 1 mes desde la notificación | Art. 13.3 Ley 6/2020 |
| Identificación previa por personación, en una relación preexistente con el prestador, que dispensa de una nueva | Menos de 5 años desde esa identificación | Art. 7.6 Ley 6/2020 |
| Periodicidad de reunión de la CETIC | Al menos trimestral | Art. 3.6 RD 1125/2024 |
| Informe de la CETIC al Consejo de Ministros sobre el estado de la transformación digital | Anual (lo trimestral es la reunión, art. 3.6) | Art. 3.4 RD 1125/2024 |
| Plazo para comunicar gestión directa al órgano jurisdiccional | 24 horas | Art. 4.6 Ley 11/2022 |
| Plazo jurisdiccional para validar la gestión directa | 48 horas | Art. 4.6 Ley 11/2022 |
| Principios específicos del ENI | 3 (cualidad integral, multidimensional, multilateral) | Art. 4 RD 4/2010 |
| Dimensiones de la interoperabilidad | 3 (organizativa, semántica, técnica) + temporal | Art. 6 RD 4/2010 |

| CONCEPTO | PLAZO / CIFRA | ARTÍCULO |
|---|---|---|
| Plazo máximo de adecuación de sistemas existentes al ENI | 48 meses desde la entrada en vigor | DT 1.ª RD 4/2010 |
| Plazo de adaptación de medios de identificación y firma | 24 meses | DT 2.ª RD 4/2010 |

**FUENTE** *Arts. 4, 7, 9, 12, 13 Ley 6/2020; arts. 3.4 y 3.6 RD 1125/2024; art. 4.6 Ley 11/2022; arts. 4, 6 y disposiciones transitorias primera y segunda RD 4/2010*

## 06 Trampas frecuentes de examen

- **Trampa: el cese del prestador «en todo caso» y la suspensión que extingue «siempre».** Lo falso que pidieron señalar: el cese en la actividad del prestador como causa de revocación **en todo caso** (2021-1A, pregunta 88; 2024-3A, pregunta 83) y que en la suspensión **la vigencia del certificado se extinguirá siempre** (2021-2B, pregunta 88). El art. 5.1.f Ley 6/2020 exceptúa el cese cuando la gestión de los certificados se transfiere a otro prestador de servicios de confianza, y el art. 5.3 solo extingue el certificado suspendido si vence el plazo de la suspensión sin que el prestador la haya levantado. Pista: busca el «salvo» y el «si».
- **Trampa: el ámbito de la Ley 6/2020.** Distractores: prestadores públicos **establecidos o no en España** y prestadores de otro Estado con servicios **supervisados** por la autoridad de otro país de la UE (2022-1A, pregunta 87), o con establecimiento **temporal** (2024-3A, pregunta 82). El art. 2 se aplica a los prestadores públicos y privados establecidos en España y a los 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.
- **Trampa: ámbito subjetivo del RD 1125/2024.** Distractor: una afirmación que extiende la norma a **CCAA y Entidades Locales**. FALSO: el art. 2 limita el ámbito a la **Administración del Estado** (AGE + organismos públicos y entidades de Derecho público vinculados).
- **Trampa: vigencia del certificado cualificado.** Distractores posibles: **3 años**, **10 años** (2022-Canarias-3A dio tres años, un año y seis meses). El art. 4.2 Ley 6/2020 establece que el período de vigencia **no será superior a cinco años**.
- **Trampa: plazo de conservación de información del prestador cualificado.** Distractor: **5 años**, que es la vigencia máxima del certificado. El art. 9.3.a Ley 6/2020 fija **15 años** desde la extinción del certificado o la finalización del servicio.
- **Trampa: red institucional de las AAPP.** Distractores: **la Red Iris** o **la red TESTA de la Unión Europea**. El art. 13.1 RD 4/2010 establece que la red de las AAPP españolas la presta la **Red**

SARA.

- **Trampa: sincronización de la hora oficial.** Distractores: **Centro Criptológico Nacional**, **Fábrica Nacional de Moneda y Timbre** o **INCIBE**. El art. 15.2 RD 4/2010 obliga a sincronizar con el **Real Instituto y Observatorio de la Armada**.
- **Trampa: ámbito de la Ley 11/2022.** Distractor: incluye **los servicios de comunicación audiovisual y los contenidos transmitidos**. FALSO: el art. 1.2 los excluye expresamente. La ley regula las redes y los servicios de comunicaciones electrónicas, sus recursos y servicios asociados, los equipos radioeléctricos y los equipos terminales (art. 1.1).
- **Trampa: la responsabilidad del cedente por errores.** Lo falso que pidieron señalar: **el cedente es responsable con respecto al cesionario en caso de errores de la aplicación** (2023-1A, pregunta 87, la que no era condición de licenciamiento). FALSO: el art. 16.1.e RD 4/2010 prevé la **ausencia total de responsabilidad por parte del cedente** en caso de errores o mal funcionamiento de la aplicación, y el 16.1.d, la **no obligación de asistencia técnica o de mantenimiento**.
- **Trampa: almacenar o copiar datos de creación de firma.** Distractor: los prestadores pueden **almacenar y copiar, por sí o a través de un tercero, los datos de creación de firma**. FALSO: art. 9.1.b Ley 6/2020 lo prohíbe, salvo gestión en nombre del titular (y entonces con sistemas y productos fiables y bajo el control exclusivo del titular).
- **Trampa: qué órgano declara los medios comunes y tiene la iniciativa de la Estrategia TIC.** Distractores: la **Dirección de Tecnologías de la Información y las Comunicaciones**, las **Comisiones Ministeriales de Administración Digital** y el **Comité de Dirección de las Tecnologías de Información y Comunicaciones** en lugar de la Comisión de Estrategia TIC para declarar los medios y servicios compartidos (2024-1A, pregunta 84, todavía con el RD 806/2014), y el **Comité de Estrategia TIC** en lugar de la Comisión para la iniciativa de la Estrategia TIC (2024-2A, pregunta 83). En el RD 1125/2024, la CETIC declara transversales determinados medios o servicios comunes, a propuesta del Consejo Rector de la Agencia (arts. 3.3.e y 9.1), y el Gobierno aprueba la Estrategia TIC a iniciativa de la CETIC y a propuesta de la persona titular del Ministerio para la Transformación Digital y de la Función Pública (art. 8). Pista: es una «Comisión», no un «Comité» ni una «Dirección».
- **Trampa: la reunión trimestral y el informe anual de la CETIC.** La Comisión se reúne **al menos, trimestralmente** (art. 3.6 RD 1125/2024), no de forma **mensual**, **semestral** ni **anual**. Lo anual es el informe sobre el estado de la transformación digital que eleva al Consejo de Ministros (art. 3.4), y 2022-Canarias-3A (pregunta 85) dio **trimestralmente** como distractor de ese informe.
- **Trampa: a quién se comunica cada cosa en el art. 60 Ley 11/2022.** Ante un **riesgo particular** de violación de la seguridad de la red o del servicio, el operador informa a los **abonados** (60.2); 2020-1A (pregunta 85) dio como falsa que informa a la **Agencia Española de Protección de Datos**. Ante una **violación de datos personales**, notifica **sin dilaciones indebidas** a la **AEPD** (60.3), no al **Centro Criptológico Nacional** ni a la **CNMC**. Los prestadores de servicios de confianza, cualificados o no, notifican además al Ministerio las

violaciones de seguridad o pérdidas de la integridad del art. 19.2 del Reglamento (UE) 910/2014 (art. 13.1 Ley 6/2020).

- **Trampa: prestadores no cualificados y verificación previa.** Distractor: los prestadores no cualificados **necesitarán verificación administrativa previa**. FALSO: art. 12 Ley 6/2020 dice que **no necesitan verificación administrativa previa**; basta comunicar al Ministerio en el plazo de tres meses.
- **Trampa: ENI vs ENS.** Distractor: confundir Esquema Nacional de Interoperabilidad (RD 4/2010, dimensiones organizativa/semántica/técnica) con el Esquema Nacional de Seguridad: 2024-2A (pregunta 85) dio el ENS en lugar del ENI para la interoperabilidad de sedes y registros (art. 25 RD 4/2010).
- **Trampa: principios específicos del ENI.** Lo falso que pidieron señalar: **la interoperabilidad como mecanismo de control** (2022-1A, pregunta 89: la que no era principio). Solo existen tres: **cualidad integral**, **carácter multidimensional**, **enfoque de soluciones multilaterales** (art. 4 RD 4/2010).
- **Trampa: quién fija la seguridad de los bienes afectos a las redes.** Distractores: el **Ministerio del Interior**, el Ministerio para la Transformación Digital y de la Función Pública o la **Secretaría de Estado de Seguridad** (2024-1A, pregunta 83). Las medidas las determina el **Gobierno**, a propuesta de los Ministerios de Defensa, del Interior o de Asuntos Económicos y Transformación Digital (art. 4.5 Ley 11/2022).
- **Trampa: los objetivos del art. 3 Ley 11/2022, deformados.** 2023-1A (pregunta 86) cambió el mercado interior por el **equilibrio entre el mercado exterior e interior**, la neutralidad tecnológica por la **neutralidad ecológica** y el servicio público por el **servicio público y privado**. La ley dice: contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea (f), fomentar la neutralidad tecnológica en la regulación (i) y garantizar el cumplimiento de las obligaciones de servicio público (j).
- **Trampa: los datos de la interceptación (art. 58.5 Ley 11/2022).** 2023-2A (pregunta 86) coló los **datos bancarios utilizados en la relación proveedor/usuario**, que la lista no incluye; sí están, entre otros, los servicios básicos utilizados, la dirección de la comunicación y la causa de finalización.
- **Trampa: el plan de clasificación (art. 21.1.e RD 4/2010).** 2023-2A (pregunta 87) dio como medida **un plan único de clasificación adaptado a las funciones generales del conjunto de las Administraciones Públicas**. El plan se adapta a las funciones, generales y específicas, de cada una de las Administraciones públicas y de sus entidades vinculadas o dependientes.
- **Trampa: los aspectos de la digitalización (art. 24.1 RD 4/2010).** 2022-Canarias-3A (pregunta 89) añadió el **tamaño del documento**. Son cuatro: formatos estándares y técnica de compresión, nivel de resolución, garantía de imagen fiel e íntegra y metadatos mínimos obligatorios y complementarios.
- **Trampa: quién aprueba las normas técnicas de interoperabilidad.** 2026-A (pregunta 83) dio la **Comisión Sectorial de Administración Electrónica**, que solo propone, la **Secretaría de Estado de Función Pública**, que publica la resolución, y el Centro de interoperabilidad

semántica. Las aprueba el **Ministerio para la Transformación Digital y de la Función Pública** (DA 1.ª.2 RD 4/2010).

- **Trampa: recomendaciones de la guía del CCN-CERT cambiadas de apartado o del revés.** 2020-2A (pregunta 84) dio como consejos de mensajería instantánea los de redes sociales (perfil y privacidad, pseudónimo, cuidado con los enlaces); el de mensajería era configurar las aplicaciones para recibir mensajes solo de personas autorizadas. 2022-2A (pregunta 88) dio la vuelta a uno del correo: **confiar únicamente en el nombre del remitente**, cuando hay que comprobar que el dominio es de confianza. 2025-A (pregunta 84) dio bitcoin como **centralizada**, con control **directo** y sin riesgo de blanqueo: el informe la describe descentralizada, con control indirecto de los usuarios y con riesgo de blanqueo y de evasión fiscal.

> **FUENTE** *Distractores de las preguntas del banco y de las convocatorias*

## 07 Reglas mnemotécnicas

- **«5-15-1.5M-2» — los plazos del prestador cualificado (Ley 6/2020): 5** años de vigencia máxima del certificado (art. 4.2); **15** años de conservación de información (art. 9.3.a); **1.500.000 €** de seguro mínimo de responsabilidad civil, salvo sector público (art. 9.3.b); **2** meses de aviso de cese (art. 9.3.c). El no cualificado solo memoriza **3** meses (art. 12) para comunicar el inicio, la modificación de datos y el cese.
- **«OST + T» — las dimensiones de la interoperabilidad (art. 6 RD 4/2010): O**rganizativa, **S**emántica, **T**écnica, y la dimensión en el **T**iempo (conservación). Las tres principales son OST; la temporal se añade aparte.
- **«PEC = CCN-CERT»:** lo **P**úblico, lo **E**stratégico y lo **C**lasificado van al **CCN-CERT**: el Sector Público, las empresas y organizaciones de interés estratégico y cualquier sistema clasificado (guía BP/01).
- **«SARA presta, ROA da la hora»:** dos pilares fáciles de confundir del ENI. **Red SARA** es quien presta la red de comunicaciones de las AAPP (art. 13); el **Real Observatorio de la Armada** (ROA) sincroniza la hora oficial (art. 15). Si la pregunta menciona red → SARA; si menciona hora → ROA.
- **«Ministro preside, F1-D2 vicepresidencias»:** CETIC. La persona titular del **Ministerio para la Transformación Digital y de la Función Pública** preside; VP**1** = SE de **F**unción Pública; VP**2** = SE de **D**igitalización e IA. Memorizar el orden numérico evita confundir las dos vicepresidencias.

> **FUENTE** *Síntesis mnemónica de los datos del tema*

## 08 Conexiones entre temas

- → **Tema 4 (Constitución):** el secreto de las comunicaciones del art. 58 Ley 11/2022 desarrolla el **art. 18.3 CE** (secreto telefónico, postal y telegráfico); las interceptaciones necesitan resolución judicial, y el **art. 55.2 CE** solo permite suspender ese secreto para personas determinadas, en investigaciones sobre bandas armadas o elementos terroristas, con la necesaria intervención judicial y el adecuado control parlamentario.
- → **Tema 10 (Derecho Administrativo, Leyes 39/2015 y 40/2015):** el ENI se estableció en el art. 42 de la antigua Ley 11/2007 y hoy lo recoge el art. 156.1 Ley 40/2015 (criterios y recomendaciones de seguridad, conservación y normalización de la información, los formatos y las aplicaciones); el art. 156.2 regula el Esquema Nacional de Seguridad. El RD 1125/2024 se aplica a la Administración del Estado: la AGE y sus organismos públicos y entidades de Derecho público vinculados o dependientes, según la Ley 40/2015 (art. 2 RD 1125/2024).
- → **Tema 11 (LOPDGDD):** el art. 60 Ley 11/2022 y el art. 8 Ley 6/2020 remiten al **RGPD (Reglamento UE 2016/679)** y a la **LO 3/2018**. La notificación de una violación de datos personales a la **AEPD** del art. 60.3 Ley 11/2022 tiene su propio plazo, «sin dilaciones indebidas», y el art. 60.4 deja a salvo la aplicación del RGPD y de la LO 3/2018, cuya autoridad de control, la AEPD, es la del Tema 11.
- → **Tema 13 (Seguridad Ciudadana / Privada):** el DNI electrónico acredita electrónicamente la identidad personal de su titular, en los términos del **art. 8 LO 4/2015**, y permite la firma electrónica de documentos (DA 3.ª Ley 6/2020).
- → **Tema 19 (Deontología Profesional):** el **deber de reserva y de secreto** del agente (art. 27 del Código de Conducta de la GC, RD 176/2022) se solapa con el **secreto de las comunicaciones** que el operador debe garantizar (art. 58 Ley 11/2022). En la práctica, un agente que accede a comunicaciones interceptadas legalmente está sujeto a ambos secretos acumulados.

> **FUENTE** *Derecho Constitucional; Derecho Administrativo; Protección de Datos; Seguridad Pública y Seguridad Privada; Deontología Profesional*