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: Octubre 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

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** y un bloque sin fuente legal directa sobre criptografía y CCN-CERT.

Peso en examen
Medio-alto: entre 2 y 5 preguntas por convocatoria 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
RD 1125/2024 art. 3 (composición de la CETIC — pregunta estrella del tema, 13+ preguntas en el banco); Ley 11/2022 arts. 4, 58 y 60 (servicios reservados, secreto e interceptación, protección de datos); Ley 6/2020 arts. 2, 4, 5, 9 y 12 (ámbito, vigencia, revocación, obligaciones de prestadores cualificados, prestadores no cualificados); ENI RD 4/2010 arts. 4, 11, 13, 15, 16, 21, 23, 24, 25 y DA 1.ª (principios, estándares, Red SARA, hora oficial, licenciamiento, conservación, digitalización).

Qué pesa más
Composición de la CETIC (presidente, dos vicepresidencias, secretario, periodicidad trimestral); el plazo de **cinco años** de vigencia de los certificados cualificados; el seguro de **1.500.000 €** + **500.000 €** adicionales; el plazo de conservación de **quince años**; los principios específicos del ENI; la **Red SARA**; el **Real Instituto y Observatorio de la Armada** como referencia de hora oficial; y la guía del **CCN-CERT** «Principios y recomendaciones básicas en Ciberseguridad», con 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** *Arts. 1-4, 56-63 Ley 11/2022; arts. 1-10 RD 1125/2024; arts. 1-13, DA 3.ª Ley 6/2020; arts. 1-29, DA 1.ª RD 4/2010 ENI; RD 421/2004 y RD 311/2022*

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).

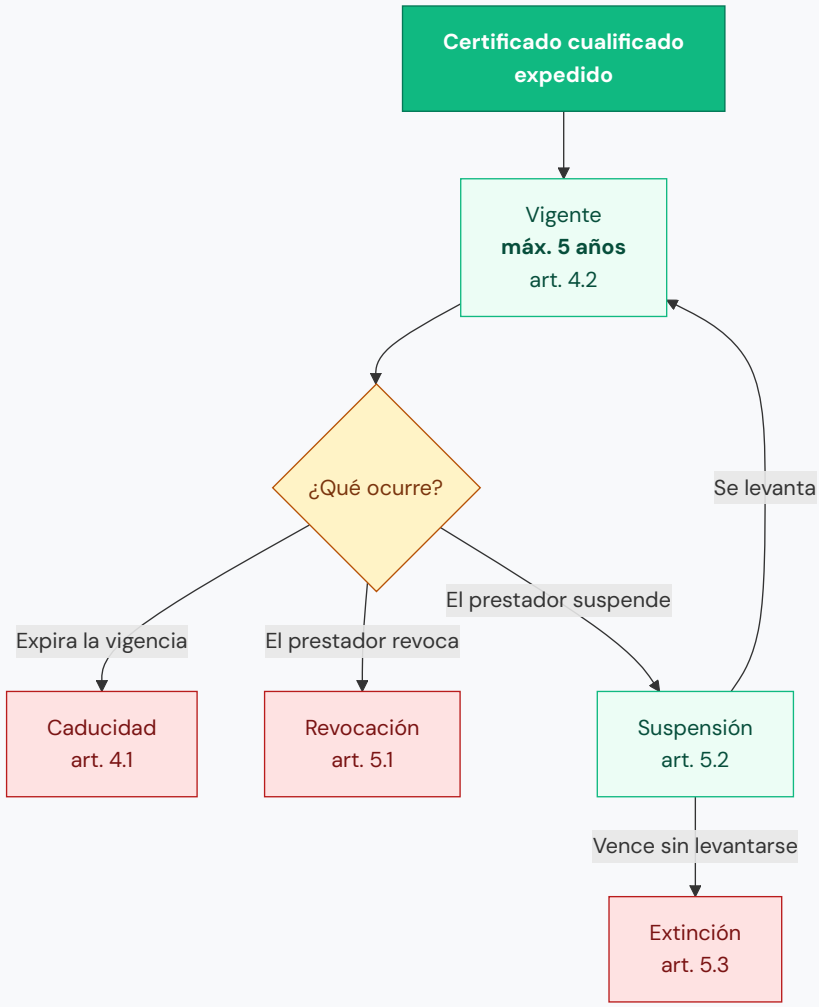

Figura 1: Vigencia, suspensión y extinción de un certificado electrónico (arts. 4 y 5 Ley 6/2020)

FUENTE *Ley 6/2020*

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 la instalación y explotación de redes y servicios de comunicaciones electrónicas (art. 149.1.21.ª CE). **Quedan excluidos:** servicios de comunicación audiovisual, contenidos transmitidos por las redes y servicios de la sociedad de la información (Ley 34/2002).
- **Art. 2.1 Ley 11/2022 — Las telecomunicaciones como servicios de interés general.** Son **servicios de interés general que se prestan en régimen de libre competencia**. Solo tienen consideración de servicio público los del art. 4 (seguridad, defensa).
- **Art. 3 Ley 11/2022 — Objetivos y principios.** Fomentar la competencia efectiva, desarrollar la economía digital, promover el despliegue de redes, garantizar la **neutralidad tecnológica**, defender los intereses de los usuarios, salvaguardar derechos fundamentales. (Cayó en oposición 2023 — apartado e: «promover el desarrollo de la ingeniería».)
- **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. El Gobierno puede acordar la asunción excepcional y transitoria de la gestión directa de servicios de comunicaciones electrónicas; el acuerdo se comunica en **24 horas** al órgano jurisdiccional, que resuelve en **48 horas**.
- **Art. 56 Ley 11/2022 — Salvaguardia de derechos fundamentales.** Las medidas restrictivas del acceso o uso solo pueden imponerse si son **adecuada, necesaria y proporcionada en una sociedad democrática** y respetan presunción de inocencia, vida privada, libertad de expresión y tutela judicial efectiva.
- **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**. Están obligados a realizar las interceptaciones autorizadas judicialmente (cap. V del título VIII libro II LECrim y LO 2/2002 control judicial del CNI). Deben facilitar al agente facultado: 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: identificación, domicilio, número de titular, número de identificación del terminal, número de cuenta del proveedor, dirección de correo. En caso de cifrado, deben entregar las comunicaciones **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; los soportes con contenidos se custodian hasta finalizar el expediente o se destruyen.
- **Art. 60 Ley 11/2022 — Protección de datos de carácter personal.** Los operadores adoptan medidas técnicas y de gestión: acceso solo personal autorizado, protección frente a destrucción y pérdida, política de seguridad. En caso de violación de datos personales notifican **sin dilaciones indebidas** a la **AEPD**; si afecta a un abonado, también al abonado, salvo medidas tecnológicas que conviertan los datos en incomprensibles.

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 art. 60.3 Ley 11/2022, los distractores frecuentes son Ministerio del Interior, CCN-CERT o INCIBE; la pista de origen es la fórmula **«sin dilaciones indebidas»** dirigida a la **AEPD**.*

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.

- **Art. 61 Ley 11/2022 — Conservación y cesión de datos.** Se rige por la Ley 25/2007.
- **Art. 62 Ley 11/2022 — Cifrado.** Puede imponerse a los operadores la obligación de facilitar a la AGE los algoritmos y aparatos de cifra en casos justificados de protección de la seguridad del Estado, seguridad pública y persecución de delitos. La información obtenida se trata con máxima confidencialidad y se destruye una vez resuelta la amenaza o firme la sentencia.
- **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. El Ministerio informa a otras autoridades nacionales, a la **ENISA** y, si procede, a la CNMC; comunica también a la Secretaría de Estado de Seguridad lo relevante para infraestructuras críticas.

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 medios y servicios comunes, declarar proyectos de interés prioritario, 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 a representantes externos con voz pero sin voto.
- **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 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 según la tecnología empleada.

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.

*Cuando el examen pregunta por art. 4.2 Ley 6/2020, los distractores frecuentes son **tres años** o **diez años**; la pista de origen es **«no será superior a cinco años»**, fijado según la tecnología empleada.*

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.

- **Art. 5 Ley 6/2020 — Revocación y suspensión.** Supuestos (entre otros): a) solicitud del firmante, representado, tercero autorizado o titular; b) puesta en peligro del secreto de los datos de creación; c) resolución judicial o administrativa; d) fallecimiento, capacidad modificada, extinción jurídica o pérdida del nombre de dominio; e) terminación de la representación; f) cese del prestador, salvo transferencia; g) falsedad o inexactitud de los datos; h) mecanismos criptográficos por debajo del estándar; i) cualquier otra causa lícita. 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 art. 5.1 Ley 6/2020, el distractor frecuente exige **resolución judicial**; la pista es que la letra a) admite la **solicitud del firmante** y la letra b) la **puesta en peligro** del secreto.*

El art. 5.1 Ley 6/2020 obliga al prestador a revocar el certificado cuando lo solicita el firmante (letra a) o cuando se ponen en peligro los datos de creación de firma por utilización indebida de un tercero (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 / vídeo-identificación con seguridad equivalente certificada por organismo de evaluación de la conformidad. La personación previa puede no exigirse si existe una identificación previa **menor de cinco años**.

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.

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

El art. 7.2 Ley 6/2020 admite 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); disponer de servicio de consulta sobre el estado de validez o revocación. 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 con **antelación mínima de dos meses** a clientes y al órgano de supervisión; 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 si el destinatario actúa con información incompleta, negligencia en la conservación de los datos de creación, no solicita la suspensión cuando duda, o utiliza el certificado tras su expiración / suspensión.
- **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).
- **Art. 13 Ley 6/2020 — Obligaciones de seguridad.** Cualificados y no cualificados notifican al Ministerio las violaciones de seguridad o pérdidas de integridad (art. 19.2 Reglamento UE 910/2014), sin perjuicio de la notificación a la AEPD. Plazo máximo de **un mes** para ampliar la información tras la notificación inicial.
- **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. (Pregunta clásica de descarte: «exclusividad territorial» o «control unilateral» NO son principios.)

- **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.** Modelos de datos comunes obligatorios, publicados a través del **Centro de Interoperabilidad Semántica de la Administración (CISA)**.
- **Art. 11 RD 4/2010 — Estándares aplicables.** Se usarán **estándares abiertos** y, complementariamente, estándares de **uso generalizado por los ciudadanos**. El uso en exclusiva de un estándar no abierto sin alternativa abierta se limita a los casos en que no exista estándar abierto que satisfaga la funcionalidad. 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, ni la red del CCN).
- **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 se justifica y se autoriza por 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: política de gestión de documentos, **índice electrónico** firmado para garantizar la integridad del expediente, identificación única e inequívoca de cada documento, **metadatos mínimos obligatorios**, plan de clasificación adaptado a las funciones, período de conservación fijado por las comisiones calificadoras, acceso completo e inmediato, conservación a lo largo del ciclo de vida, formación tecnológica del personal.
- **Art. 22 RD 4/2010 — Seguridad.** Aplica el ENS (RD 311/2022) para conservación; integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad.
- **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, los distractores frecuentes omiten alguno de los cuatro elementos; 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 para inscribir a su hija en el colegio público. 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 sede y el registro electrónicos se rigen por el **ENI**; el distractor frecuente coloca en su lugar el ENS o una norma autonómica.*

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…). En materia de **ciberseguridad y criptografía**, 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).** Lo regula el **RD 421/2004**, de 12 de marzo: está adscrito al CNI (art. 2.3) y lo dirige el Secretario de Estado Director del CNI (art. 1). Entre sus funciones (art. 2.2): elaborar y difundir normas, instrucciones, guías y recomendaciones de seguridad TIC para la Administración (las guías **CCN-STIC**, DA 2.ª RD 311/2022), formar al personal especialista de la Administración, ser el organismo de certificación de la seguridad de productos y sistemas TIC y velar por el cumplimiento de la normativa sobre información clasificada. Su capacidad de respuesta a incidentes es el **CCN-CERT**. La guía BP/01 cita tres herramientas del CCN-CERT: **LUCIA** (notificación de ciberincidentes, pág. 52), **PILAR** (análisis de riesgos, pág. 40) y **MARIA** (análisis de código dañino con varios antivirus, pág. 17).
- **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. Para los operadores de servicios esenciales, su comunidad de referencia son las entidades del ámbito de la Ley 40/2015 (art. 11.1.a RDL 12/2018), y en los casos de especial gravedad coordina la respuesta técnica de los CSIRT (art. 11.2). Su sistema de detección es el Sistema de Alerta Temprana (SAT INET y SAT SARA, guía BP/01, pág. 51).
- **INCIBE-CERT.** Equipo de respuesta del Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad mercantil estatal bajo la tutela del Ministerio para la Transformación Digital y de la Función Pública (art. 6.8 RD 210/2024). Es el CSIRT de referencia de los **ciudadanos**, las **entidades de derecho privado** y las demás entidades no asignadas a otro equipo (art. 11.1 RDL 12/2018); con los operadores críticos, lo operan juntos el INCIBE y el CNPIC (art. 11.1.a.2.º).
- **ESPDEF-CERT.** Capacidad de respuesta del Mando Conjunto del Ciberespacio, del Ministerio de **Defensa**: es la referencia para el ámbito de la Defensa Nacional (art. 33.4 RD 311/2022) y coopera con el CCN-CERT y el INCIBE-CERT cuando estos lo requieran y, necesariamente, en los operadores que tengan incidencia en la Defensa Nacional (art. 11.1.a.3.º RDL 12/2018).
- **RD 311/2022 — Esquema Nacional de Seguridad (ENS).** Aplica a todo el sector público; categoriza los sistemas en **BÁSICA**, **MEDIA** y **ALTA**. Cinco dimensiones de seguridad: **confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad**. Diferencia clave con RD 1125/2024: el ENS aplica a todo el sector público; el RD 1125/2024 solo a la Administración del Estado.
- **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.

- **Tipos de malware.** Virus, gusanos (worms), troyanos, ransomware, spyware, adware, rootkits, keyloggers, botnets.
- **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.

FUENTE *Arts. 1-4, 56-63 Ley 11/2022; arts. 1-10 RD 1125/2024; arts. 1-13, DA 3.ª Ley 6/2020; arts. 1-29, DA 1.ª RD 4/2010; RD 421/2004; RD 311/2022; guía CCN-CERT; RDL 12/2018; RD 210/2024*

04 Tablas comparativas

Tabla 1 — CERTs nacionales: a quién atiende cada uno.

CERT	ADSCRIPCIÓN	A QUIÉN ATIENDE	FUENTE / HERRAMIENTAS
CCN-CERT	Centro Criptológico Nacional, adscrito al CNI (art. 2.3 RD 421/2004)	Sector Público, empresas y organizaciones de interés estratégico y cualquier sistema clasificado (guía BP/01, pág. 4); para los operadores de servicios esenciales, las entidades del ámbito de la Ley 40/2015 (art. 11.1.a RDL 12/2018)	Guía BP/01; art. 11 RDL 12/2018; art. 33 RD 311/2022; herramientas LUCIA, PILAR y MARIA; guías CCN-STIC
INCIBE-CERT	INCIBE, sociedad mercantil estatal bajo la tutela del Ministerio para la Transformación Digital y de la Función Pública (art. 6.8 RD 210/2024)	Ciudadanos, entidades de derecho privado y demás entidades no asignadas a otro equipo (art. 11.1 RDL 12/2018)	Art. 11.1 RDL 12/2018; con el CNPIC para los operadores críticos (art. 11.1.a.2.º)
ESPDEF-CERT	Mando Conjunto del Ciberespacio, Ministerio de Defensa (art. 33.4 RD 311/2022)	Ámbito de la Defensa Nacional; coopera con los otros dos y, necesariamente, en los operadores con incidencia en la Defensa Nacional (art. 11.1.a.3.º RDL 12/2018)	Art. 33.4 RD 311/2022; art. 11.1.a.3.º RDL 12/2018

Tabla 2 — 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. 20 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	1.500.000 € (+ 500.000 € por servicio adicional, art. 9.3.b)
Aviso de cese	Comunicación al Ministerio	2 meses de antelación a clientes y Ministerio (art. 9.3.c)

Tabla 3 — RD 4/2010 ENI vs RD 311/2022 ENS.

ASPECTO	ENI (RD 4/2010)	ENS (RD 311/2022)
Objeto	Interoperabilidad organizativa, semántica y técnica	Seguridad de la información en el sector público
Ámbito subjetivo	Sector público (art. 2 Ley 11/2007)	Todo el sector público
Dimensiones	Organizativa, semántica, técnica y temporal	Confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad
Categorización	No aplica	Básica, media, alta
Norma técnica de referencia	Normas técnicas DA 1.ª; CISA; EUPL	Guías CCN-STIC del CCN
Red institucional	Red SARA (art. 13)	No regula ninguna; la respuesta a incidentes se articula en torno al CCN-CERT (art. 33)

Tabla 4 — 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 5 — 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 *RD 421/2004; guía CCN-CERT; RDL 12/2018; RD 210/2024; arts. 9, 12 Ley 6/2020; RD 4/2010 ENI; RD 311/2022 ENS; 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 de responsabilidad civil (prestador cualificado)	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 válida sin personación nueva	Menor de 5 años	Art. 7.6 Ley 6/2020
Periodicidad de reunión de la CETIC	Al menos trimestral	Art. 3.6 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
Categorías ENS (RD 311/2022)	3 (básica, media, alta)	RD 311/2022
Dimensiones de seguridad del ENS	5 (CIDAT)	RD 311/2022
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; art. 3.6 RD 1125/2024; art. 4.6 Ley 11/2022; arts. 4, 6 + DT 1.ª, 2.ª RD 4/2010; RD 311/2022*

06 Trampas frecuentes de examen

- **Trampa: ámbito subjetivo del RD 1125/2024.** El examen presenta como correcta 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). Para todo el sector público se aplica el ENS (RD 311/2022), no el RD 1125/2024.
- **Trampa: vigencia del certificado cualificado.** Distractores frecuentes: **3 años**, **10 años**. 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.** Distractores: **5 años** (coincidente con la vigencia máxima), **10 años**. 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 típicos: **Red IRIS** (es de I+D, no AAPP), **plataforma Cl@ve** (es de identificación, no es la red), **red del CCN-CERT**. 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: **Instituto Geográfico Nacional**, **Centro Criptológico Nacional**. 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 (art. 149.1.27.ª CE). Solo redes y servicios de comunicaciones electrónicas.
- **Trampa: obligación de prestar asistencia técnica.** Distractor: el cedente está **obligado a prestar asistencia técnica permanente y mantenimiento**. FALSO: art. 16.1.d RD 4/2010 establece 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: vicepresidencias de la CETIC intercambiadas.** El examen invierte la VP1 y la VP2 de la CETIC. La pista clave: VP1 = SE de **Función Pública**; VP2 = SE de **Digitalización e Inteligencia Artificial**. Fíjate en el cargo, no en el orden de las siglas.
- **Trampa: periodicidad de la CETIC.** Distractores: **mensual**, **semestral**, **anual**. El art. 3.6 RD 1125/2024 establece **al menos, trimestralmente**.
- **Trampa: comunicación tras incidente de seguridad de datos personales.** Distractor: notificar al **Ministerio del Interior** o al **CCN**. El art. 60.3 Ley 11/2022 obliga a notificar a la **AEPD** (Agencia Española de Protección de Datos). Si además es prestador cualificado de servicios de confianza, art. 13 Ley 6/2020 obliga también a comunicar al Ministerio competente.
- **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 Esquema Nacional de Seguridad (RD 311/2022, dimensiones **CIDAT**: Confidencialidad, Integridad, Disponibilidad, Autenticidad, Trazabilidad).
- **Trampa: principios específicos del ENI.** Distractores en la lista de los 3 principios: **principio de exclusividad territorial**, **control unilateral**, **soberanía tecnológica**. Solo existen tres: **cualidad integral**, **carácter multidimensional**, **enfoque de soluciones multilaterales** (art. 4 RD 4/2010).

> **FUENTE** *Distractores reales de tema-17.json + convocatorias 2022-2025; arts. clave Ley 11/2022, RD 1125/2024, Ley 6/2020, RD 4/2010*

07 Reglas mnemotécnicas

- **«5-15-1.5M-2» — los plazos del prestador cualificado (Ley 6/2020): 5** años de vigencia del certificado (art. 4.2); **15** años de conservación de información (art. 9.3.a); **1.500.000 €** de seguro de responsabilidad civil (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.
- **«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.

- **«CIDAT» — las 5 dimensiones de seguridad del ENS (RD 311/2022): C**onfidencialidad, **I**ntegridad, **D**isponibilidad, **A**utenticidad, **T**razabilidad. (Aviso: las dimensiones del ENI son distintas — OST + tiempo, no CIDAT.)
- **«LUCIA notifica, PILAR analiza, MARIA escanea»: las tres herramientas del CCN-CERT que cita la guía BP/01. LUCIA**, la notificación formal del ciberincidente; **PILAR**, el análisis de riesgos; **MARIA**, el análisis de código dañino con varios antivirus.
- **«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). Los ciudadanos y las entidades de derecho privado, al **INCIBE-CERT** (art. 11.1 RDL 12/2018); el ámbito de la Defensa Nacional, al **ESPDEF-CERT**, que además coopera con los dos.
- **«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.
- **«Ministra preside, F1-D2 vicepresidencias»:** CETIC. La 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 el distractor de invertir las vicepresidencias.

> **FUENTE** *Mnemónicas basadas en arts. 3-12 Ley 6/2020; arts. 4, 6, 13, 15 RD 4/2010; art. 3 RD 1125/2024; RD 311/2022; guía CCN-CERT; RDL 12/2018*

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 requieren autorización judicial salvo en el supuesto del **art. 55.2 CE** (suspensión individual). El DNI electrónico (DA 3.ª Ley 6/2020) materializa el derecho a la identidad personal.
- **→ Tema 10 (Derecho Administrativo, Leyes 39/2015 y 40/2015):** el ENI desarrolla el art. 42 de la antigua Ley 11/2007 (hoy art. 156 Ley 40/2015). El RD 1125/2024 organiza la AGE conforme al art. 2 Ley 40/2015. La **Red SARA** es la red que sustenta los procedimientos administrativos electrónicos del art. 14 Ley 39/2015 (obligación de relación electrónica).
- **→ 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 violación de datos del art. 60.3 Ley 11/2022 a la **AEPD** sigue el régimen del art. 33 RGPD (72 horas) y se complementa con la sanción de los arts. 73-83 LOPDGDD.

- **→ Tema 13 (Seguridad Ciudadana / Privada):** el DNI electrónico (DA 3.ª Ley 6/2020) remite al **art. 8 LO 4/2015**. La intervención de las telecomunicaciones por servicios técnicos (art. 59 Ley 11/2022) se coordina con las funciones de la GC como Policía Judicial.
- **→ Tema 19 (Deontología Profesional):** el **secreto profesional** del agente (art. 6 RD 176/2022 Código de Conducta GC) 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 *Cross-refs T4, T10, T11, T13, T19*