GUARDIA CIVIL: ESQUEMA TEMA 17
MATERIAS TÉCNICO-CIENTÍFICAS. TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

opositu.com

Ley 11/2022 + RD 1125/2024 + Ley 6/2020 + RD 4/2010 ENI ~52 artículos Edición: Mayo 2026

ESTRUCTURA DEL BLOQUE XVI · 4 NORMAS

A	Ley 11/2022 General de Telecomunicaciones	arts. 1-4, 56-63	B	RD 1125/2024 Administración Digital AGE	arts. 1-10
C	Ley 6/2020 Servicios Electrónicos de Confianza	arts. 1-13 + DA 3.ª	D	RD 4/2010 Esquema Nacional de Interoperabilidad	arts. 1-29 + DA 1.ª

BLOQUES COLATERALES SIN FUENTE LEGAL DIRECTA (TAMBIÉN CAEN)

E1	Criptografía simétrica / asimétrica / hash	AES · RSA · SHA-256	E2	CCN-CERT / INCIBE-CERT / ESPDEF-CERT	RD 421/2004
E3	ENS (Esquema Nacional de Seguridad)	RD 311/2022	E4	Malware · Red TOR · Pirámide del daño	guías CCN-STIC

CARACTERÍSTICAS CLAVE DEL BLOQUE TIC

4	~52	3-5	30	0,8
normas vigentes	artículos clave	preguntas/conv. desde 2022	preg. ley analizadas (2017-2025)	peso medio-alto

CRONOLOGÍA DE LAS NORMAS TIC

2004-05-12	**RD 421/2004** crea el **Centro Criptológico Nacional (CCN)**, adscrito al CNI.
2010-01-29	**RD 4/2010 ENI** — Esquema Nacional de Interoperabilidad (art. 42 Ley 11/2007, hoy Ley 40/2015).
2014-07-23	RD 806/2014 organización TIC en AGE (DEROGADO por RD 1125/2024).
2020-11-12	**Ley 6/2020** — Servicios electrónicos de confianza (complemento del Reglamento UE 910/2014 «eIDAS»).
2022-05-04	**RD 311/2022 ENS** — Esquema Nacional de Seguridad (5 dimensiones CIDAT).
2022-06-29	**Ley 11/2022** General de Telecomunicaciones (deroga Ley 9/2014).
2024-11-05	**RD 1125/2024** — nueva gobernanza TIC en la Administración del Estado (deroga RD 806/2014).

ARTICULADO · LAS 4 NORMAS (VERBATIM BOE)

A · LEY 11/2022 GENERAL DE TELECOMUNICACIONES (TÍTULO I · OBJETO Y PRINCIPIOS)

Art. 1 **Objeto y ámbito.** Regula la instalación y explotación de redes y servicios de comunicaciones electrónicas (art. 149.1.21.ª CE). **Excluidos:** servicios de comunicación audiovisual, contenidos transmitidos y servicios de la sociedad de la información (trampa: incluir audiovisual).

Art. 2.1 **Telecomunicaciones como servicios de interés general.** Son servicios de interés general que se prestan en régimen de libre competencia . Solo son servicio público los del art. 4 (defensa y seguridad).

Art. 3 **Objetivos y principios.** Fomentar la competencia efectiva , desarrollar la economía digital, garantizar la neutralidad tecnológica , defender los intereses de los usuarios y salvaguardar derechos fundamentales. **Visto 2023:** apartado e) «promover el desarrollo de la ingeniería , así como de la industria de productos y equipos de telecomunicaciones».

Art. 4 ★ **Servicios para seguridad nacional, defensa, seguridad pública, vial y protección civil.** Las redes/servicios para actividades esenciales se reservan al Estado y se rigen por su normativa específica. El Gobierno puede acordar la **asunción excepcional y transitoria** de la gestión directa; el acuerdo se comunica en **24 horas** al órgano jurisdiccional, que resuelve en **48 horas**. *Visto 2024: bienes muebles/inmuebles afectos = los califica el Gobierno.*

CAP. III · SECRETO Y SEGURIDAD DE LAS COMUNICACIONES

Art. 56 **Salvaguardia de derechos fundamentales.** Las medidas restrictivas solo si son adecuada, necesaria y proporcionada en una sociedad democrática y respetan presunción de inocencia, vida privada, libertad de expresión y tutela judicial.

Art. 57 **No discriminación.** Sin condiciones distintas por nacionalidad, residencia o lugar de establecimiento, salvo que se justifique de forma objetiva .

Art. 58 ★ **Secreto de las comunicaciones.** Conforme a los artículos 18.3 y 55.2 de la Constitución . Obliga a interceptaciones autorizadas judicialmente (LECrim + LO 2/2002 CNI). Facilitar al agente: identidad de las partes, servicios, dirección, causa de finalización, marcas temporales, localización. En cifrado: entregar comunicaciones desprovistas de los efectos , con calidad no inferior a la del destinatario. *Visto 2023: no se facilitan datos bancarios* .

Art. 59 **Interceptación por servicios técnicos.** Control del dominio radioeléctrico / localización de interferencias; soportes con contenidos se custodian o destruyen al cerrar expediente.

Art. 60 ★ **Protección de datos personales.** Política de seguridad; acceso solo personal autorizado. Notificar sin dilaciones indebidas a la **AEPD** (y al abonado afectado), salvo medidas tecnológicas que hagan los datos incomprensibles. No al Ministerio del Interior · no al CCN .

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

Art. 62 **Cifrado.** Puede imponerse facilitar a la AGE algoritmos y aparatos de cifra (seguridad del Estado, seguridad pública, persecución de delitos). Máxima confidencialidad; destrucción tras amenaza resuelta o sentencia firme.

Art. 63 **Integridad y seguridad de redes.** Notificar incidentes con impacto significativo al Ministerio. Parámetros: nº usuarios afectados, duración, área geográfica, funcionamiento, alcance económico y social. Se informa a ENISA y, si procede, a la CNMC.

B · RD 1125/2024 ADMINISTRACIÓN DIGITAL AGE (DEROGA RD 806/2014, 5-NOV-2024)

Art. 1 **Objeto.** Desarrollo de un modelo común de gobernanza de las TIC en la AGE y sus organismos públicos y entidades de Derecho público vinculados; incluye la **Estrategia TIC** y la mejora de los servicios públicos.

Art. 3.6 **Periodicidad.** Se reúne al menos, trimestralmente ; la convoca la presidencia, que puede invitar a representantes externos con voz pero sin voto. NO mensual · NO semestral · NO anual (anual = el informe al Consejo de Ministros).

Art. 2 **Ámbito.** Administración del Estado : AGE + organismos públicos y entidades de Derecho público vinculados o dependientes (Ley 40/2015). NO alcanza a CCAA ni EELL (para todo el sector público → ENS).

Art. 3 ★ **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; **VP 1.ª** = SE de **Función Pública**; **VP 2.ª** = SE de **Digitalización e Inteligencia Artificial**; vocales: Dirección de la Agencia Estatal de Administración Digital, un representante por cada ministerio (Subsecretaría), D.G. Gobernanza Pública, representante de la Abogacía General del Estado, que actuará con voz pero sin voto ; secretario = titular de la Secretaría General de la Agencia.

Art. 3.3 **Funciones CETIC.** Fijar líneas estratégicas, aprobar la propuesta de Estrategia TIC, informar anteproyectos TIC, prioridades de inversión, **declarar transversales** medios y servicios, **declarar proyectos prioritarios**, informar proyectos sectoriales, impulsar colaboración con CCAA/EELL. *Visto 2024: declarar transversales corresponde a la CETIC.*

Art. 8 **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 ★ **Medios y servicios digitales comunes transversales.** Los declara **transversales la CETIC** a propuesta del Consejo Rector de la Agencia cuando respondan a necesidades de un número significativo de unidades. Uso de carácter obligatorio y sustitutivo respecto a medios particulares. La Agencia elabora el **Catálogo de Medios y Servicios Comunes**.

Art. 10 **Proyectos de interés prioritario.** Singular relevancia (colaboración con CCAA, EELL, UE); la declaración se traslada como **recomendación al Consejo de Ministros** para tenerla en cuenta en los PGE.

C · LEY 6/2020 SERVICIOS ELECTRÓNICOS DE CONFIANZA (COMPLEMENTO EIDAS REG. UE 910/2014)

Art. 1 **Objeto.** Complemento del **Reglamento (UE) 910/2014 «eIDAS»**.

Art. 2 ★ **Ámbito.** Prestadores públicos y privados establecidos en España y prestadores residentes o domiciliados en otro Estado con establecimiento permanente situado en España , si ofrecen servicios no supervisados por la autoridad de otro Estado UE. *Visto 2022 + 2024.*

Art. 3 **Efectos jurídicos.** Prueba: no cualificado (art. 326.3 LEC); cualificado (art. 326.4 LEC).

Art. 4 ★ **Vigencia y caducidad.** Los certificados se extinguen por **caducidad** o **revocación**. Período de vigencia de cualificados no será superior a cinco años , fijado según la tecnología empleada. NO 3 años · NO 10 años · NO seis meses .

Art. 5 ★ **Revocación y suspensión.** Supuestos: a) solicitud del firmante; b) puesta en peligro del secreto; 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 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 de b)/g).

Art. 6 **Identidad del titular.** Persona física: nombre, apellidos y **DNI/NIE/NIF** (o pseudónimo). Persona jurídica: denominación o razón social y NIF.

Art. 7 **Comprobación de identidad.** Regla general: personación ante los encargados; acreditación con DNI, pasaporte u otros medios. Excepción: firma legitimada notarialmente, o vídeo-identificación equivalente certificada. Personación previa puede no exigirse si existe identificación previa menor de cinco años .

Art. 8 **Datos personales.** Pseudónimos: el prestador conserva la documentación real y la revela a órganos judiciales y autoridades públicas habilitadas.

Art. 9 ★ **Obligaciones de los prestadores.** Generales: publicar información veraz; No almacenar ni copiar , por sí o tercero, los datos de creación de firma/sello/autenticación, salvo gestión en nombre del titular (con sistemas fiables); servicio de consulta sobre validez/revocación. **Adicionales cualificados (art. 9.3):** a) conservar información **15 años** desde la extinción del certificado o la finalización del servicio prestado ; b) seguro RC mínimo **1.500.000 €** (no sector público) + **500.000 €** por cada tipo de servicio adicional; c) comunicar cese con antelación mínima de dos meses ; d) remitir informe de conformidad (art. 20.1 Reg. UE 910/2014).

Art. 10 **Responsabilidad.** Asumen toda la responsabilidad frente a terceros por personas o prestadores en los que deleguen, incluida la comprobación de identidad previa.

Art. 11 **Limitaciones.** No responde si el destinatario actúa con información incompleta, negligencia en custodia, no pide suspensión cuando duda, o usa el certificado tras expiración / suspensión.

Art. 12 ★ **Inicio de servicios no cualificados.** no necesitan verificación administrativa previa ; basta comunicar al Ministerio en plazo de **tres meses** desde el inicio. El Ministerio publica el listado en lista **separada** de la cualificada. *Visto 2025.*

Art. 13 **Obligaciones de seguridad.** Notificar al Ministerio violaciones de seguridad o pérdidas de integridad (art. 19.2 Reg. UE 910/2014), sin perjuicio de la AEPD. Plazo máximo **un mes** para ampliar información tras la notificación inicial.

DA 3.ª **DNI electrónico.** Acredita electrónicamente la identidad (art. 8 LO 4/2015) y permite la firma. Lo expide el **Ministerio del Interior**; sus órganos asumen las obligaciones de prestador cualificado.

D · RD 4/2010 ESQUEMA NACIONAL DE INTEROPERABILIDAD (DE 8 DE ENERO)

Art. 1 **Objeto.** Regula el ENI establecido en el **art. 42 Ley 11/2007** (hoy art. 156 Ley 40/2015). Criterios y recomendaciones para garantizar la interoperabilidad organizativa, semántica y técnica.

Art. 2 **Definiciones.** Remite al Glosario de Términos incluido en el anexo .

Art. 3 **Ámbito.** El del art. 2 Ley 11/2007. El ENI y sus normas de desarrollo prevalecerán sobre cualquier otro criterio en materia de política de interoperabilidad.

Art. 4 ★ **Principios específicos.** Tres: a) La interoperabilidad como cualidad integral ; b) Carácter multidimensional de la interoperabilidad ; c) Enfoque de soluciones multilaterales . NO «mecanismo de control» · NO «exclusividad territorial» · NO «soberanía tecnológica» . *Visto 2022 (1A + Canarias-3A).*

Art. 5 **Cualidad integral.** La interoperabilidad se tiene presente desde la concepción y a lo largo de su **ciclo de vida**: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión.

Art. 6 **Carácter multidimensional.** Dimensiones organizativa, semántica y técnica (más la dimensión temporal de conservación).

Art. 7 **Enfoque multilateral.** Aproximación multilateral para obtener ventajas del escalado, arquitecturas modulares y multiplataforma, compartir,

Art. 12 **Infraestructuras y servicios comunes.** Las AAPP enlazarán sus infraestructuras con las comunes de la AGE.

Art. 13 ★ **Red de comunicaciones.** Las AAPP utilizan preferentemente la **Red de comunicaciones AAPP españolas**, prestada por la Red SARA . NO Red IRIS · NO Cl@ve · NO red del CCN .

Art. 14 **Plan de direccionamiento.** Aplican el Plan de direccionamiento e interconexión de redes.

Art. 15 ★ **Hora oficial.** Sincronización con precisión que garantice la certidumbre de los plazos . Sincroniza con el Real Instituto y Observatorio de la Armada (RD 1308/1992) y, cuando sea posible, con la hora oficial europea. NO IGN · NO CCN .

Art. 16 ★ **Licenciamiento.** Aplicaciones públicas con: a) reutilización de recursos; b) protección frente a apropiación exclusiva; c) exención de responsabilidad del cedente por mal uso; d) no obligación de asistencia técnica o de mantenimiento ; e) ausencia de responsabilidad por errores; f) licenciamiento por defecto sin contraprestación. Fuentes abiertas: ejecución, conocimiento, modificación y redistribución. Preferencia: **EUPL**. *Visto 2023: cedente NO responsable de errores.*

reutilizar y colaborar.

Arts. 8-9 **Interoperabilidad organizativa.** Servicios por medios electrónicos: condiciones publicadas; uso de la **Red de comunicaciones AAPP**; nodos de interoperabilidad. Inventarios: procedimientos (SIA) y órganos/oficinas (**Directorio Común DIR3**).

Art. 10 **Interoperabilidad semántica.** Modelos de datos comunes obligatorios, publicados a través del **CISA** (Centro de Interoperabilidad Semántica de la Administración).

Art. 11 **Estándares aplicables.** estándares abiertos y, complementariamente, estándares de uso generalizado por los ciudadanos. El uso exclusivo de un estándar no abierto solo si no existe abierto que satisfaga la funcionalidad. Criterios: especificaciones TIC (Reg. UE 1025/2012), formalización, coste, madurez y reutilización.

Arts. 17-18 **Directorios + firma.** AGE mantiene el Directorio general (**Centro de Transferencia de Tecnología**, art. 158 Ley 40/2015). La AGE define la política marco de firma; no aplicación se justifica y autoriza por la SGAD.

Art. 20 **Plataformas de validación.** Servicios de confianza en un único punto de llamada; incorporan las listas de confianza nacionales y europeas.

Art. 21 ★ **Recuperación y conservación.** Política de gestión, índice electrónico firmado, identificación única de cada documento, metadatos mínimos obligatorios, plan de clasificación **adaptado a las funciones** (NO «plan único común»), período de conservación fijado por comisiones calificadoras, acceso completo, formación tecnológica.

Art. 22 **Seguridad.** Aplica el **ENS (RD 311/2022)** para integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad.

Art. 23 ★ **Formatos.** Conservar el documento en el formato en que se elaboró/recibió y, preferentemente, en estándar abierto que preserve a lo largo del tiempo contenido, firma y metadatos. Si riesgo de obsolescencia: copiado auténtico con cambio de formato.

Art. 24 ★ **Digitalización de papel.** Formatos estándares, técnica de compresión, nivel de resolución, garantía de imagen fiel e íntegra, metadatos obligatorios y complementarios. NO «tamaño del documento».

Art. 25 ★ **Sedes y registros electrónicos.** Su interoperabilidad y la del acceso electrónico se rige por el **ENI**. *Visto 2024: NO ENS · NO SIA · NO Comité Sectorial.*

Arts. 26-29 **Conformidad + actualización.** Inclusión en el ciclo de vida; controles en cada órgano; publicidad de las declaraciones en sedes electrónicas. El ENI se desarrolla en paralelo al progreso de la Administración Electrónica.

DA 1.ª ★ **Desarrollo del ENI.** Normas técnicas obligatorias (Catálogo de estándares, Documento electrónico, Digitalización, Expediente, Política de firma, Protocolos, Modelos de datos, Política de gestión, Requisitos de conexión, Copiado auténtico, Reutilización…). **Ciberseguridad y criptografía:** órgano competente el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia. *Visto 2025.*

3 PRINCIPIOS ESPECÍFICOS ENI (ART. 4) + 5 DIMENSIONES DE SEGURIDAD ENS «CIDAT»

1	2	3	C	I	D	A	T
Cualidad integral todo el ciclo de vida	**Carácter multidimensional** organiz. + sem. + técn.	**Soluciones multilaterales** escalado, modular, multiplataforma	**Confidencialidad** ENS dim. 1	**Integridad** ENS dim. 2	**Disponibilidad** ENS dim. 3	**Autenticidad** ENS dim. 4	**Trazabilidad** ENS dim. 5

CIFRAS CLAVE DEL BLOQUE TIC

5 años vigencia certificado cualificado (art. 4.2 L 6/2020)	**15 años** conservación información (art. 9.3.a L 6/2020)	**1,5 M€** seguro RC prestador cualif. (art. 9.3.b)	**500 K€** suplemento por servicio adicional (art. 9.3.b)	**2 meses** antelación aviso de cese (art. 9.3.c)	**3 meses** comunicar inicio no cualif. (art. 12 L 6/2020)
1 mes ampliar info tras incidente (art. 13.3)	**<5 años** identificación previa válida sin nueva personación (art. 7.6)	**Trim.** periodicidad CETIC (art. 3.6 RD 1125/2024)	**24 h** comunicar gestión directa al juez (art. 4.6 L 11/2022)	**48 h** resolución jurisdiccional (art. 4.6 L 11/2022)	**3** categorías ENS: básica · media · alta
5 dimensiones ENS «CIDAT»	**3 + 1** dimensiones ENI (org. sem. téc. + temporal)	**48 m** adecuación sistemas ENI (DT 1.ª RD 4/2010)	**24 m** adaptación medios id./firma (DT 2.ª RD 4/2010)		

HOTSPOTS EXAMEN GC (PREGUNTAS-LEY 2017-2025)

8 Ley 6/2020 — arts. 2, 4, 5, 9, 12	**7** RD 4/2010 ENI — arts. 4, 16, 21, 23, 24, 25, DA 1.ª	**5** CCN-CERT (TOR, pirámide, bitcoin, correo, móvil)	**4** RD 1125/2024 / 806/2014 — arts. 3, 4, 9, 12
4 Ley 11/2022 — arts. 3, 4, 58			

CERTS NACIONALES · ¿A QUIÉN ATIENDE CADA UNO?

CERT	ADSCRIPCIÓN	ATIENDE A
CCN-CERT	Centro Criptológico Nacional (CNI) · *RD 421/2004*	**Sector público (AGE, CCAA, EELL)**
INCIBE-CERT	Instituto Nacional de Ciberseguridad	**Empresas privadas y ciudadanos**
ESPDEF-CERT	Ministerio de Defensa	**Fuerzas Armadas y Defensa**

SERVICIOS DE CONFIANZA · CUALIFICADOS VS NO CUALIFICADOS

ASPECTO	NO CUALIFICADOS	CUALIFICADOS
Inicio actividad	Sin verificación previa (art. 12)	**Verificación + evaluación conformidad**
Comunic. Ministerio	3 meses desde inicio	Antes del inicio
Lista pública	Lista separada	Lista de confianza (TSL)
Conservación info	No fijado	**15 años desde extinción**
Seguro RC	No exigido	**1,5 M€ + 500 K€/serv. adicional**
Aviso cese	Comunicar al Ministerio	**2 meses antelación**

ENI (RD 4/2010) VS ENS (RD 311/2022)

ASPECTO	ENI	ENS
Objeto	Interoperabilidad	Seguridad de la información
Ámbito	Sector público (art. 2 L 11/2007)	Todo el sector público
Dimensiones	Org. · sem. · técn. (+ temporal)	**CIDAT (5)**

ASPECTO	ENI	ENS
Categorización	No aplica	**Básica · media · alta**
Red institucional	**Red SARA (art. 13)**	SAT del CCN-CERT

CRIPTOGRAFÍA · SIMÉTRICA VS ASIMÉTRICA VS HASH

TIPO	CLAVES	USO TÍPICO	ALGORITMOS
Simétrica	Una compartida	Grandes volúmenes	AES, 3DES, RC4
Asimétrica	Pública + privada	**Firma electrónica**	RSA, ECC, ElGamal
Hash	Ninguna (unidireccional)	Integridad / huella	SHA-256, SHA-3

14 TRAMPAS FRECUENTES DE EXAMEN GC

Art. 2 RD 1125 ~~extiende a CCAA y EELL~~ → **solo Administración del Estado** (AGE + organismos vinculados).
Para todo el sector público → ENS (RD 311/2022), no este RD.

Art. 4.2 L 6/2020 ~~3 años · 10 años · 6 meses~~ → **cinco años** de vigencia máxima de cualificados.
Visto en 2022 Canarias-3A + 2021-2B.

Art. 9.3.a L 6/2020 ~~5 años · 10 años~~ de conservación → **15 años** desde extinción/finalización.
No confundir con la vigencia (5 años) — son plazos distintos.

CCN-CERT ~~atiende a empresas y ciudadanos privados~~ → **eso lo hace el INCIBE-CERT**. CCN-CERT = sector público.
«Sector privado → INCIBE; sector público → CCN.»

Art. 13 ENI ~~Red IRIS · Cl@ve · red del CCN~~ → **Red SARA** presta la red de comunicaciones AAPP.
IRIS = I+D. Cl@ve = identificación. CCN = ciberseguridad.

Art. 15 ENI ~~Instituto Geográfico Nacional · CCN~~ → **Real Instituto y Observatorio de la Armada** sincroniza la hora oficial.
«SARA presta la red, ROA da la hora.»

Art. 1 L 11/2022 ~~incluye servicios audiovisuales y contenidos transmitidos~~ → **EXCLUIDOS** expresamente (art. 1.2). Solo redes y servicios de comunicaciones electrónicas.
Visto en 2020-1A.

Art. 16 ENI ~~obligación de asistencia técnica permanente y mantenimiento~~ → **no obligación de asistencia técnica o de mantenimiento**.
Apartado d) del licenciamiento. Visto en 2023-1A.

Art. 9.1.b L 6/2020 ~~deberán almacenar y copiar los datos de creación de firma~~ → **NO almacenar ni copiar**.
Excepción única: gestión en nombre del titular, con sistemas fiables. Visto en 2024-2A.

CETIC VPs VP1 y VP2 ~~intercambiadas~~ → **VP1 = Función Pública · VP2 = Digitalización e IA**.
«F-1, D-2» — orden numérico.

Art. 3.6 RD 1125 ~~mensual · semestral · anual~~ → **al menos, trimestralmente**.
Anual = el informe al Consejo de Ministros, no la reunión.

Art. 60.3 L 11/2022 Notificar incidente datos al ~~Ministerio del Interior · CCN~~ → **AEPD**.
Si además es prestador cualificado → también al Ministerio competente (art. 13 L 6/2020).

Art. 12 L 6/2020 No cualificados ~~necesitan verificación administrativa previa~~ → **no necesitan verificación administrativa previa**; basta comunicar al Ministerio en 3 meses.
Visto en 2025-A.

Art. 4 ENI 3 principios → ~~exclusividad territorial · control unilateral · soberanía tecnológica · mecanismo de control~~ NO son principios → **cualidad integral · multidimensional · soluciones multilaterales**.
Visto en 2022-1A y Canarias-3A.

REGLAS MNEMOTÉCNICAS

5-15-1,5M-2

Cualificado L 6/2020: 5 años vigencia · **15** años conservación · **1,5 M€** seguro · **2** meses aviso cese. (No cualificado: solo **3** meses para comunicar inicio.)

O · S · T + T

Dimensiones ENI (art. 6): Organizativa, **S**emántica, **T**écnica + dimensión en el **T**iempo. OST son las tres; la temporal va aparte.

CIDAT

5 dimensiones ENS (RD 311/2022): Confidencialidad · **I**ntegridad · **D**isponibilidad · **A**utenticidad · **T**razabilidad. ENI ≠ ENS (OST ≠ CIDAT).

LUCIA · PILAR · CLARA

Herramientas CCN-CERT: LUCIA abre el incidente · **PILAR** analiza el riesgo · **CLARA** audita la configuración.

SECTOR → CERT

Routing de incidentes: sector **público** → **CCN-CERT** · **privado/ciudadano** → **INCIBE-CERT** · **Defensa/FAS** → **ESPDEF-CERT**.

SARA presta · ROA da la hora

Confusión ENI clásica: art. 13 → **Red SARA** presta la red AAPP. Art. 15 → **Real Observatorio de la Armada** sincroniza la hora.

F-1 · D-2

CETIC VPs (art. 3.2 RD 1125): Ministra preside · VP**1** = SE de **F**unción Pública · VP**2** = SE de **D**igitalización e IA.

24-48

Gestión directa redes seguridad (art. 4.6 L 11/2022): Gobierno comunica al juez en **24 h**; el juez resuelve en **48 h**.

DATOS CLAVE CIBERSEGURIDAD · SIN FUENTE LEGAL DIRECTA

RD 421/2004 crea el Centro Criptológico Nacional (CCN), adscrito al CNI. Misión: certificar productos TIC, formar AAPP, gestionar el CCN-CERT, redactar las **Guías CCN-STIC**.

RD 311/2022 ENS aplica a todo el sector público. Categoriza sistemas en **BÁSICA · MEDIA · ALTA**. 5 dimensiones CIDAT. Distinción vs RD 1125/2024 (solo Administración del Estado).

Red TOR — anonimato; origen: investigación de la Marina de los Estados Unidos (US Naval Research Laboratory). *Visto 2024-1A.*

Pirámide del daño CCN-CERT: en el vértice superior las acciones patrocinadas por Estados (mayor capacidad + más recursos). *Visto 2024-3A.*

Bitcoin (CCN-CERT): en lugar de acuñar moneda se usa una cadena de caracteres criptográficos intercambiados en «billeteras». **BlockChain** registra las transacciones. *Visto 2025-A.*

Hash criptográfico (SHA-256, SHA-3): propiedades = **unidireccionalidad**, **resistencia a colisiones**, **determinismo**.

Tipos de malware: virus, gusanos, troyanos, ransomware, spyware, adware, rootkits, keyloggers, botnets.

Correo seguro (CCN-CERT): verificar el dominio completo del remitente, no fiarse del icono adjunto, no habilitar macros. *Visto 2022-2A.*

CONEXIONES ENTRE TEMAS

T4 **Constitución:** el secreto 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**.

T4 El **DNI electrónico** (DA 3.ª Ley 6/2020) materializa el derecho a la identidad personal del art. 18.4 CE.

T10 **Derecho Administrativo:** 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.

T10 La **Red SARA** sustenta los procedimientos administrativos electrónicos del **art. 14 Ley 39/2015** (obligación de relación electrónica).

T11 **LOPDGDD:** el art. 60 Ley 11/2022 y el art. 8 Ley 6/2020 remiten al **RGPD (Reg. UE 2016/679)** y a la **LO 3/2018**. La notificación a la AEPD del art. 60.3 sigue el régimen del art. 33 RGPD (72 horas).

T13 **Seguridad Ciudadana:** el DNI electrónico (DA 3.ª Ley 6/2020) remite al **art. 8 LO 4/2015**. La intervención de telecomunicaciones por servicios técnicos (art. 59 Ley 11/2022) se coordina con las funciones de GC como Policía Judicial.

T19 **Deontología:** el **secreto profesional** del agente (art. 6 RD 176/2022 Código de Conducta GC) se suma al **secreto de las comunicaciones** del operador (art. 58 Ley 11/2022) cuando el agente accede a interceptaciones legales.

CÓMO USAR ESTE ESQUEMA

Un vistazo no basta. Úsalo así.

1. **Lee el esquema entero.** Por lo menos una vez, para ver de qué va el tema y cómo encaja todo.

2. **Tápalo y recuerda.** Cubre cada bloque e intenta reconstruirlo de memoria. Lo que no te salga, eso es justo lo que falta repasar.

3. **Repaso de última hora.** Tenlo a mano los días previos al examen. Para refrescar la memoria, un esquema vale más que releer el temario entero.

4. **Demuestra que te lo sabes.** El examen es tipo test; entrénate 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.