TEMA 1: LA SOCIEDAD DE LA INFORMACIÓN. IDENTIDAD Y FIRMA ELECTRÓNICA: RÉGIMEN JURÍDICO. EL DNI ELECTRÓNICO. LA AGENDA DIGITAL PARA ESPAÑA.

Cuerpo de Técnicos Auxiliares de Informática de la Administración del Estado · I. Administración electrónica y transparencia

1. Marco Normativo e Introducción

El marco jurídico de la Sociedad de la Información y la administración digital se fundamenta en los mandatos de eficacia y modernización del artículo 103 de la Constitución Española. A nivel europeo y estatal, este ecosistema se vertebra mediante la Directiva 2000/31/CE y la Ley 34/2002 (LSSI-CE), junto con el estándar de confianza digital establecido por el Reglamento (UE) 910/2014 (eIDAS) y la Ley 6/2020 de servicios electrónicos de confianza, complementados por los artículos 9 y 10 de la Ley 39/2015 (LPACAP) para el sector público.

2. La sociedad de la información

Marco conceptual y principios rectores de la LSSI-CE (Ley 34/2002)

La Ley 34/2002 regula los servicios de la sociedad de la información y la contratación electrónica, transponiendo la normativa comunitaria del mercado digital.

Establece el régimen de obligaciones de los prestadores establecidos en España y la libre prestación transfronteriza de servicios dentro de la Unión Europea.

- Principio de no autorización previa: la prestación de servicios no está sujeta a autorización específica previa administrativa.
- Deber de información general (Art. 10): obligación de acceso permanente, fácil y gratuito a datos identificativos (nombre/razón social, NIF, domicilio, datos registrales, precios con desglose impositivo y gastos de envío).
- Comunicaciones comerciales por vía electrónica (Art. 21): prohibición expresa del envío publicitario no solicitado (spam) sin consentimiento previo del destinatario (régimen opt-in), salvo relación contractual previa con productos similares.
- Régimen de cookies y almacenamiento de datos (Art. 22.2): exigencia de información clara y completa sobre su utilización y obtención del consentimiento informado previo del usuario antes de su instalación.

> **Atención Opositor:** *El principio de libre prestación de servicios solo puede restringirse judicial o administrativamente por motivos de orden público, salud pública, seguridad nacional o protección de los consumidores y menores.*

Régimen de responsabilidad de los prestadores de servicios de intermediación

La normativa exime a los intermediarios técnicos de una obligación general de supervisar los datos que transmiten o almacenan activamente.

La exención de responsabilidad civil, penal y administrativa está estrictamente condicionada a la pasividad y neutralidad técnica del intermediario.

- Operadores de redes y mero transporte ('mere conduit', Art. 14): no responden por el contenido transmitido si no originan la transmisión, no seleccionan al destinatario y no modifican los datos.
- Copia temporal o memoria caché ('caching', Art. 15): exención condicionada a no manipular la información, respetar las condiciones de acceso y retirarla con prontitud cuando el emisor original la haya eliminado.
- Alojamiento de datos o 'hosting' (Art. 16): exención total salvo que el prestador tenga conocimiento efectivo de la ilicitud del contenido o, teniéndolo, no actúe con diligencia debida para retirar o bloquear el acceso al mismo.
- Concepto legal de conocimiento efectivo: cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o bloqueo, y el prestador conozca dicha resolución administrativa o judicial.

> **Atención Opositor:** *No existe para los prestadores de intermediación una obligación general de supervisión de contenidos ni de búsqueda activa de hechos o circunstancias que indiquen actividades ilícitas.*

Régimen sancionador de la Ley 34/2002

La potestad sancionadora recae en el Ministerio competente en materia digital y, en su caso, en la Agencia Española de Protección de Datos (AEPD).

La ley tipifica tres niveles de infracción con sus correspondientes límites cuantitativos y plazos de prescripción extintiva.

- Infracciones muy graves: incumplimiento reiterado de órdenes de bloqueo de contenidos o vulneración de medidas cautelares (multas de 150.001 a 600.000 euros; prescripción a los 3 años).
- Infracciones graves: envío masivo de spam publicitario no consentido, no facilitar información identificativa sustancial o incumplimiento del régimen de cookies (multas de 30.001 a 150.000 euros; prescripción a los 2 años).
- Infracciones leves: no inclusión de datos registrales o identificativos menores en la web o comunicaciones (multas de hasta 30.000 euros; prescripción al año).
- Competencia sancionadora de la AEPD: tutela específica de infracciones vinculadas al envío no consentido de spam (Art. 21) y uso indebido de cookies (Art. 22.2).

3. Identidad y firma electrónica: régimen jurídico

Régimen normativo: Reglamento eIDAS (UE 910/2014) y Ley 6/2020

El Reglamento (UE) 910/2014 (eIDAS) unifica el marco comunitario de identificación electrónica y servicios de confianza en las transacciones del mercado interior.

La Ley 6/2020 derogó la antigua Ley 59/2003 de firma electrónica, adaptando el marco nacional estrictamente a las competencias reservadas por el reglamento europeo.

- Servicios electrónicos de confianza: expedición de certificados de firma y sello, sellado de tiempo, servicios de entrega electrónica certificada y autenticación de sitios web.
- Prestador de servicios cualificado: entidad auditada y supervisada que cumple los rigurosos requisitos del Reglamento eIDAS y figura en la Lista de Confianza (TSL) nacional.
- Listas de Confianza (TSL): registros públicos gestionados por los Estados miembros que confieren certeza jurídica transfronteriza a los prestadores y servicios cualificados.
- Eficacia jurídica general: a ningún efecto probatorio puede denegarse eficacia o validez a una firma por el simple hecho de presentarse en formato digital o no ser cualificada.

> **Atención Opositor:** *La Ley 6/2020 regula aspectos residuales no armonizados por eIDAS: comprobación de la identidad para certificados cualificados (presencial o por identificación remota por vídeo autorizada), conservación temporal de registros y régimen de infracciones.*

Tipología de firmas electrónicas y efectos jurídicos según el Reglamento eIDAS

El ordenamiento jurídico comunitario clasifica la firma electrónica en tres niveles progresivos de seguridad y exigencia técnica.

La distinción técnica repercute directamente en la carga probatoria procesal y la equivalencia material con el soporte papel tradicional.

- Requisitos de la firma electrónica avanzada (Art. 26 eIDAS): estar vinculada al firmante de manera única, permitir la identificación del firmante, haber sido creada con datos de creación bajo control exclusivo del firmante y garantizar la integridad de los datos frente a modificaciones posteriores.
- Requisitos de la firma electrónica cualificada: debe ser una firma avanzada creada mediante un Dispositivo Cualificado de Creación de Firma (QSCD) y basarse en un Certificado Cualificado de Firma Electrónica.
- Efecto legal privilegiado: la firma electrónica cualificada tiene una equivalencia jurídica automática y plena a la firma manuscrita tradicional (Art. 25.2 eIDAS).
- Reconocimiento transfronterizo: una firma cualificada generada con un certificado expedido en cualquier Estado miembro de la UE debe ser reconocida obligatoriamente como tal en todos los demás Estados miembros.

Tipo de Firma	Base Técnica	Dispositivo Requerido	Equivalencia Manuscrita
Firma Electrónica Simple	Datos en formato electrónico asociados a otros datos electrónicos (ej. PIN, checkbox, login)	No requiere dispositivo homologado	No equivale a firma manuscrita (valor probatorio libre)
Firma Electrónica Avanzada	Cumple los 4 requisitos del Art. 26 eIDAS (control exclusivo, integridad, identificación, unicidad)	No requiere dispositivo cualificado específico	No equivale a firma manuscrita (admisión procesal con inversión de carga probatoria)

Firma Electrónica Cualificada	Firma avanzada basada en certificado cualificado emitido por prestador de confianza acreditado	Obligatorio Dispositivo Cualificado de Creación de Firma (QSCD)	Equivalencia plena legal y automática a la firma manuscrita (Art. 25.2 eIDAS)

> **Atención Opositor:** *En caso de litigio civil o administrativo sobre una firma cualificada, la carga de la prueba recae sobre quien la impugne si se demuestra que el certificado figuraba en la lista de confianza (TSL) y no estaba revocado.*

Identificación y firma electrónica en las Administraciones Públicas (Ley 39/2015)

La Ley 39/2015 separa conceptualmente la mera identificación electrónica de los interesados (Art. 9) del acto formal de firma electrónica para manifestar voluntad jurídica (Art. 10).

Las Administraciones deben admitir sistemas basados en certificados electrónicos, sellos electrónicos o claves concertadas previamente registradas.

- Identificación de los interesados (Art. 9 LPACAP): basta para interactuar con la Administración en consultas, descarga de información o recepción de notificaciones generales.
- Firma de los interesados (Art. 10.2 LPACAP): obligatoria para formular solicitudes, presentar declaraciones responsables o comunicaciones, interponer recursos, desistir de acciones y renunciar a derechos.
- Sistemas de firma admitidos por la AGE: sistemas de firma cualificada/avanzada basados en certificados reconocidos, sellos electrónicos para personas jurídicas y sistemas de clave concertada (ej. Cl@ve Firma, Cl@ve PIN) validados por el Estado.
- Firma por funcionario público habilitado (Art. 12 LPACAP): permite la identificación y firma electrónica a ciudadanos no dotados de medios digitales mediante consentimiento expreso para el trámite presencial.
- Sellos electrónicos de las Administraciones Públicas (Art. 40 Ley 40/2015): firma electrónica cualificada aplicada para la actuación administrativa automatizada sin intervención humana directa.

> **Atención Opositor:** *Con carácter general, para cualquier trámite no recogido taxativamente en el artículo 10.2 de la Ley 39/2015 basta la mera identificación del interesado, siendo la firma exigible únicamente para actos con trascendencia jurídica dispositiva.*

4. El DNI electrónico

Marco normativo y naturaleza jurídica

El Documento Nacional de Identidad electrónico es el documento público que acredita de forma auténtica la personalidad y nacionalidad de su titular en el ámbito físico y telemático.

Su régimen jurídico básico descansa en la Ley Orgánica 4/2015 de protección de la seguridad ciudadana y el Real Decreto 1553/2006, adaptado al marco de identificación del Reglamento (UE) 910/2014 (eIDAS) y la Ley 6/2020.

- Naturaleza jurídica: documento público oficial, personal e intransferible expedido exclusivamente por la Dirección General de la Policía (Ministerio del Interior).
- Efectos de la firma: la firma electrónica realizada con el DNIe tiene respecto de los datos consignados de forma electrónica el mismo valor jurídico que la firma manuscrita.
- Capacidad de identificación: permite la acreditación fehaciente de la identidad de la persona física en cualquier procedimiento administrativo o transacción privada online.
- Vigencia del soporte físico: 2 años (menores de 5 años), 5 años (hasta los 30 años), 10 años (hasta los 70 años) y con carácter permanente (mayores de 70 años o incapacitados).

> **Atención Opositor:** *La pérdida de validez del soporte físico del DNI extingue automáticamente la vigencia de los certificados electrónicos incorporados, pero la revocación o caducidad de los certificados no afecta a la validez física del documento.*

Estructura criptográfica y certificados incorporados

El chip criptográfico integrado en el DNIe almacena datos biométricos, la imagen digitalizada del titular y los certificados electrónicos cualificados emitidos por la Dirección General de la Policía como prestador cualificado.

Dispone de una zona de lectura visual, una zona de lectura mecánica (MRZ) y circuitos integrados que garantizan la confidencialidad, autenticidad e integridad.

- Certificado de Autenticación: asegura electrónicamente la identidad del ciudadano frente a terceros al iniciar sesión telemática o tramitaciones seguras.
- Certificado de Firma: cualificado para emitir firma electrónica con equivalencia jurídica directa a la firma manuscrita para actos, trámites y contratos.
- Certificado de la Autoridad de Certificación (AC): cadena de confianza que permite verificar las firmas expedidas por la Dirección General de la Policía.
- Periodo de validez de certificados: un máximo de 5 años (renovables en Puntos de Actualización del DNIe en comisarías sin cambiar el soporte físico).
- Mecanismos de acceso: PIN personal para operaciones privadas y PUK para desbloqueo por intentos erróneos reiterados.

Característica	Certificado de Autenticación	Certificado de Firma Electrónica
Finalidad técnica	Comprobar fehacientemente la identidad digital del titular	Vincular inequívocamente al titular con una declaración de voluntad o documento
Equivalencia jurídica	Identificación electrónica cualificada (eIDAS)	Firma electrónica cualificada equiparada a firma manuscrita
Uso no repudiable	No garantiza de forma intrínseca el no repudio de contenidos	Garantiza plenamente el no repudio del documento firmado
Activación operativa	Requiere introducción previa del PIN en el canal seguro	Requiere confirmación explícita e introducción del PIN

> **Atención Opositor:** *Los certificados del DNI electrónico son cualificados y se encuentran asociados exclusivamente a una persona física; no admiten representaciones orgánicas ni sustituyen certificados de persona jurídica o representante.*

Evolución tecnológica: DNIe 3.0 y DNI Europeo 4.0

La tecnología del DNIe ha evolucionado para responder a los estándares internacionales de movilidad y seguridad de la Unión Europea.

Las sucesivas iteraciones han eliminado progresivamente la dependencia de lectores de contacto físicos para fomentar el uso móvil.

- DNIe 3.0 (2015): incorpora interfaz dual (contacto y tecnología inalámbrica NFC bajo norma ISO/IEC 14443), permitiendo el uso directo con teléfonos inteligentes y tablets.
- DNI 4.0 o DNI Europeo (2021): adaptado al Reglamento (UE) 2019/1157 sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión.
- Modificaciones de seguridad en DNI 4.0: inclusión del código de país de dos letras (ES) en una bandera europea rodeada de doce estrellas amarillas y microchip con arquitectura de seguridad reforzada.
- Integración con MiDNI: base tecnológica orientada al uso del permiso de conducir e identidad en el smartphone con reconocimiento interoperable en toda la UE.

5. La Agenda Digital para España

Evolución estratégica: de la Agenda Digital a España Digital 2026

La Agenda Digital para España fue aprobada en febrero de 2013 como el marco paraguas alineado con la Estrategia Europa 2020 para impulsar la Sociedad de la Información.

Actualmente ha sido sucedida por la estrategia España Digital 2025 y su actualización España Digital 2026, vinculada a los fondos Next Generation EU y al PRTR.

- Evolución histórica: el enfoque inicial centrado en infraestructuras TIC tradicionales mutó hacia la digitalización profunda, ciberseguridad, soberanía del dato e Inteligencia Artificial.
- Financiación: dotada prioritariamente mediante el Mecanismo de Recuperación y Resiliencia (MRR) del Plan de Recuperación, Transformación y Resiliencia (Componentes 11 a 16).
- Objetivo tractor: alcanzar el 80% de la población con competencias digitales básicas y garantizar cobertura de banda ancha ultrarrápida del 100% de la población.

> **Atención Opositor:** *España Digital 2026 articula 10 ejes estratégicos estructurados operativamente mediante planes sectoriales, planes de choque y PERTEs (Proyectos Estratégicos para la Recuperación y Transformación Económica).*

Ejes estratégicos de España Digital 2026

La estrategia fija metas cuantificables a corto y medio plazo para consolidar a España en los primeros puestos del Índice DESI de la Comisión Europea.

Abarca desde el despliegue de redes hasta la transformación radical del sector público y las empresas.

- Eje 01 - Conectividad digital: cobertura de 100 Mbps para el 100% de la población (Plan Único) y erradicación de la brecha digital territorial.
- Eje 02 - Impulso del 5G: liderazgo europeo en corredores 5G y liberación continuada de bandas prioritarias (700 MHz, 3.5 GHz y 26 GHz).
- Eje 03 - Competencias digitales: Plan Nacional de Competencias Digitales (capacitación de ciudadanía, reducción de brecha de género y fomento de especialistas TIC).
- Eje 04 - Ciberseguridad: fortalecimiento de capacidades del CCN-CERT, INCIBE y las infraestructuras críticas del país.
- Eje 05 - Transformación de la AGE y AAPP: Plan de Digitalización de las AAPP 2021-2026 centrado en servicios públicos hiperconectados, Carpeta Ciudadana y analítica del dato.
- Eje 06 - Digitalización empresarial y Pymes: programa Kit Digital (mecanismos de bono digital) y fomento de scale-ups innovadoras.
- Eje 07 - Sector audiovisual: Plan 'Spain Audiovisual Hub' para convertir a España en plataforma europea de producción audiovisual y videojuegos.
- Eje 08 - Economía del dato e Inteligencia Artificial: Estrategia Nacional de Inteligencia Artificial (ENIA) y creación de la Agencia Española de Supervisión de la IA (AESIA).
- Eje 09 - Microelectrónica y semiconductores: desarrollo del PERTE Chip para dotar de autonomía estratégica industrial a nivel nacional y de la UE.
- Eje 10 - Derechos digitales: Carta de Derechos Digitales para la salvaguarda de garantías constitucionales en entornos digitales.

Eje / Plan Derivado	Órgano / Entidad Responsable	Meta Específica Principal
Plan de Digitalización de las AAPP	Secretaría General de Administración Digital (SGAD)	50% de servicios públicos digitales disponibles vía móvil y Carpeta Ciudadana personalizada
Plan Kit Digital	Red.es	Implantación de soluciones digitales en más de un millón de pymes y autónomos
Estrategia Nacional de Ciberseguridad	INCIBE / CCN-CNI	Despliegue del Centro de Operaciones de Ciberseguridad (SOC) de la Administración General del Estado
Estrategia Nacional de IA (ENIA)	Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA)	Creación de espacios de datos compartidos y puesta en marcha de la AESIA

> **Atención Opositor:** *La Carta de Derechos Digitales aprobada en julio de 2021 carece de rango normativo vinculante formal, pero actúa como marco deontológico y guía hermenéutica de referencia para desarrollos legislativos.*

6. Claves para el Examen

Análisis sistemático de trampas semánticas, plazos críticos y distinciones determinantes para las pruebas de selección:

Trampas habituales de los tribunales

- El DNIe no contiene una firma 'avanzada' básica, sino una firma electrónica 'cualificada', que posee por mandato del Reglamento eIDAS equivalencia plena con la firma manuscrita.
- Los certificados electrónicos del DNIe caducan a los 5 años como máximo, mientras que el soporte físico puede tener una vigencia de 5, 10 años o permanente; el tribunal suele invertir la relación de plazos.
- La Carta de Derechos Digitales no es un texto normativo con rango de ley ordinaria u orgánica; no crea nuevos tipos de recursos judiciales directos ni altera por sí misma el ordenamiento sustantivo.
- El programa Kit Digital financia paquetes de digitalización estandarizados a fondo perdido mediante bono digital concedido a la empresa, pero el pago efectivo se liquida al 'agente digitalizador adherido', no en metálico libre a la pyme.

Plazos críticos de obligada memorización

- Validez máxima de los certificados del chip del DNI: 5 años.
- Vigencia física del DNI: 2 años (menores de 5 años), 5 años (entre 5 y 30 años), 10 años (entre 30 y 70 años) y permanente (mayores de 70 años o personas en situación de gran dependencia).
- Plazo temporal del Plan de Digitalización de las Administraciones Públicas: periodo 2021-2026.
- Horizonte de los Fondos Next Generation EU y del PRTR para la ejecución de proyectos de la Agenda España Digital: 2026.

Artículos clave y preguntas frecuentes

- Art. 156 del Real Decreto 1553/2006 (en concordancia con Ley Orgánica 4/2015, art. 8): competencia exclusiva de la Dirección General de la Policía para la expedición y custodia de datos del DNI.
- Art. 25 y 26 del Reglamento (UE) 910/2014 (eIDAS): efectos jurídicos de las firmas electrónicas cualificadas y presunción legal de integridad y autoría.
- Art. 6 de la Ley 6/2020: régimen legal de los certificados cualificados de firma electrónica y obligaciones de comprobación de identidad del solicitante.
- Art. 11 de la Ley 39/2015: supuestos en los que es obligatorio exigir el uso de firma electrónica cualificada o avanzada por la Administración (desistir de acciones, renunciar a derechos, interponer recursos o presentar declaraciones responsables).

Distinciones conceptuales finas

- Certificado de Autenticación vs Certificado de Firma del DNIe: el de autenticación prueba identidad ante servidores telemáticos pero carece de presunción de firma de acuerdos sustantivos; el de firma genera una manifestación jurídica formal con no repudio vinculante.

- Tecnología DNIe 3.0 vs DNI Europeo 4.0: el 3.0 incorporó NFC y chip dual; el 4.0 adaptó la morfología gráfica exterior e interior al Reglamento (UE) 2019/1157 exigiendo el recuadro con la bandera europea y el indicativo 'ES'.
- Agenda Digital para España 2013 vs España Digital 2026: la primera se basaba en la transposición de la Agenda Digital Europea bajo la Estrategia 2020; la segunda es un plan tractor omnicomprensivo financiado por los Fondos Next Generation EU y el Plan de Recuperación.

7. Cuadro Resumen Esquemático

Concepto / Epígrafe	Fundamento Legal (Art. y Ley)	Elementos Clave / Plazos / Mayorías	Clave para Examen
Sociedad de la Información y Comercio Electrónico	Ley 34/2002 (LSSI-CE)	Obligación de información previa y retención de datos de tráfico (derogada en retención masiva según TJUE)	Régimen de exención de responsabilidad de prestadores intermediarios: no responsabilidad si no tienen conocimiento efectivo de la ilicitud
Régimen de Firma Electrónica	Reglamento (UE) 910/2014 (eIDAS) y Ley 6/2020	Tres niveles: simple, avanzada y cualificada; validez comunitaria de los servicios cualificados de confianza	La firma cualificada es la única que tiene presunción legal absoluta de equiparación con la firma manuscrita
DNI Electrónico (Estructura y Validez)	Ley Orgánica 4/2015 y Real Decreto 1553/2006	Soporte físico: 2, 5, 10 años o permanente; Certificados chip criptográfico: vigencia máxima de 5 años	Expedido exclusivamente por la DGP; la caducidad física arrastra a los certificados, pero no al revés
DNIe Tecnologías 3.0 y 4.0	Reglamento (UE) 2019/1157 y normas ISO/IEC	Uso dual contacto/contactless (NFC 14443) y bandera UE con código ES en DNI 4.0	Permite autenticación y firma mediante dispositivos móviles sin requerir lector de tarjetas inteligente externo
España Digital 2026	Estrategia España Digital y Componentes 11-16 PRTR	10 ejes estratégicos: 5G, ciberseguridad, competencias digitales, IA y digitalización pública	El Plan de Digitalización de las AAPP fija como hito que el 50% de servicios públicos sean accesibles vía Carpeta Ciudadana