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

Cuerpo de Gestión de Sistemas e Informática de la Administración del Estado · I. Administración electrónica y políticas públicas de igualdad, dependencia y transparencia

1. Marco Normativo e Introducción

El régimen de la sociedad de la información y la identificación electrónica en España se fundamenta en la garantía de los derechos digitales y la eficacia administrativa. Este marco integra el mandato constitucional del artículo 18.4 de la Constitución Española con la Directiva 2000/31/CE, la Ley 34/2002 (LSSI-CE), la Ley 6/2020 de servicios electrónicos de confianza y los artículos 9 a 11 de la Ley 39/2015 (LPACAP).

2. La sociedad de la información

Concepto, fundamentos y pilares esenciales

La sociedad de la información define el estadio socioeconómico donde la creación, distribución y manipulación de información son actividades económicas y culturales determinantes.

- Pilar de conectividad: Despliegue de redes de banda ancha ultrarrápida y tecnología 5G.
- Pilar de capital humano: Adquisición de competencias digitales ciudadanas y capacitación de especialistas TIC.
- Pilar de servicios y contenidos: Fomento de la Administración electrónica, el comercio electrónico y la economía del dato.
- Pilar de ciberseguridad y confianza: Protección de infraestructuras críticas, privacidad y resiliencia digital.

> **Atención Opositor:** *El artículo 18.4 de la Constitución Española actúa como cláusula de salvaguarda limitadora del uso de la informática para garantizar el honor y la intimidad de los ciudadanos.*

Régimen jurídico de la Ley 34/2002 (LSSI-CE)

La Ley 34/2002 transpone la Directiva 2000/31/CE sobre comercio electrónico y articula el régimen de obligaciones y responsabilidades de los prestadores de servicios de la sociedad de la información.

- Ámbito de aplicación: Prestadores establecidos en España o cuyos servicios se dirijan específicamente a territorio nacional.
- Principio de libre prestación: No sujeción a autorización previa para el inicio de la actividad de servicios de la sociedad de la información.

- Obligaciones de información (Art. 10): Identificación registral, NIF, datos de contacto, colegiación y precios con desglose tributario.
- Régimen de intermediarios: Exención de responsabilidad para operadores de red, almacenamiento en caché y alojamiento de datos, condicionada al desconocimiento efectivo de ilicitud o retirada inmediata tras conocimiento.
- Comunicaciones comerciales (Art. 21): Prohibición expresa de envíos publicitarios sin solicitud o consentimiento previo expreso (spam), salvo relación contractual previa con productos similares.
- Régimen sancionador: Clasificación en infracciones leves (hasta 30.000 euros), graves (de 30.001 a 150.000 euros) y muy graves (de 150.001 a 600.000 euros).

3. La Agenda Digital para España

Evolución histórica de los planes de digitalización

La planificación estratégica estatal en materia tecnológica ha evolucionado de planes de conectividad básica hacia la transformación digital integral y el gobierno del dato.

- Iniciativa Info XXI (2001-2003): Primer impulso institucional centrado en dotación de equipamiento e infraestructuras.
- Plan España.es (2004-2005): Orientación al fomento del acceso a Internet y la inclusión digital.
- Plan Avanza y Plan Avanza 2 (2005-2012): Despliegue masivo de banda ancha e implantación de los derechos de la Ley 11/2007 (LAECSP).
- Agenda Digital para España (2013): Alineamiento directo con la Agenda Digital para Europa 2020 de la Comisión Europea.

Marco estratégico actual: España Digital y Plan de Digitalización de las AAPP

La estrategia actual se articula en la Agenda España Digital (horizontes 2025 y 2026), financiada mediante el Componente 11 del Plan de Recuperación, Transformación y Resiliencia (PRTR).

- Alineación con la Década Digital Europea 2030: Objetivos cuantitativos en capacidades digitales, infraestructuras, empresas y servicios públicos.
- Eje 1: Conectividad digital plena y eliminación de la brecha digital territorial (objetivo 100% de cobertura de 100 Mbps).
- Eje 2: Impulso a la tecnología 5G transfronteriza y corredores de transporte.
- Eje 3: Competencias digitales ciudadanas y laborales (Plan Nacional de Competencias Digitales).
- Eje 4: Ciberseguridad reforzada mediante el INCIBE y el CCN-CERT.
- Eje 5: Transformación digital del sector público (Plan de Digitalización de las AAPP 2021-2025) bajo los principios de App-First, Cloud-First e interconexión mediante plataformas comunes (Cl@ve, Notifica, FACe, Carpeta Ciudadana).
- Eje 6: Inteligencia Artificial y Economía del Dato: Implementación de la Estrategia Nacional de Inteligencia Artificial (ENIA) y creación de la AESIA.

Plan Estratégico	Horizonte Temporal	Objetivo Principal	Instrumento Clave / Impacto AAPP
Agenda Digital para España	2013-2015	Cumplimiento de objetivos europeos TIC 2020 y desarrollo de la economía digital	Consolidación de redes ultrarrápidas y administración electrónica inicial
Plan de Digitalización de las AAPP	2021-2025	Modernización integral de la AGE, CCAA y EELL bajo arquitectura digital orientada al dato	Carpeta Ciudadana, factoría de software común, migración cloud y servicios proactivos
España Digital 2026	2020-2026	Transformación digital del modelo productivo y cohesión social/territorial	Inversión masiva ligada al PRTR (NextGenerationEU), 5G, IA y ciberseguridad nacional

> **Atención Opositor:** *El Plan de Digitalización de las Administraciones Públicas 2021-2025 moviliza una inversión superior a 3.100 millones de euros mediante el Componente 11 del PRTR.*

4. Identidad y firma electrónica: régimen jurídico

Marco normativo nacional: Ley 6/2020

La Ley 6/2020, de 11 de noviembre, derogó íntegramente la Ley 59/2003 de firma electrónica, adaptando el derecho interno al Reglamento (UE) 910/2014 (eIDAS).

- Finalidad: Complementar el Reglamento eIDAS en materias reservadas al ordenamiento de los Estados miembros.
- Servicios electrónicos de confianza: Regula expedición de certificados, sellado de tiempo, servicios de entrega electrónica certificada y autenticación de sitios web.
- Comprobación de identidad: Permite métodos alternativos a la presencia física para certificados cualificados (identificación remota por vídeo con condiciones de seguridad auditadas).
- Documentos públicos electrónicos: Otorga valor de documento público a los formalizados con firma electrónica cualificada conforme al artículo 326 de la Ley 1/2000 (LEC).
- Eficacia probatoria: La firma cualificada se equipara a la manuscrita; si se impugna una firma cualificada, la carga de la prueba recae sobre quien realiza la impugnación.
- Régimen de supervisión: Atribuido al Ministerio para la Transformación Digital y de la Función Pública como organismo de supervisión.

> **Atención Opositor:** *La Ley 6/2020 suprime la categoría histórica de firma electrónica de empresas o personas jurídicas, canalizándola hacia los sellos electrónicos o representaciones.*

Régimen en el procedimiento administrativo: Ley 39/2015 y Ley 40/2015

La legislación básica diferencia nítidamente entre los mecanismos de mera identificación y aquellos que constituyen acreditación de la voluntad mediante firma.

- Identificación ciudadana (Art. 9 Ley 39/2015): Obligatoria en todo trámite. Admite sistemas basados en certificados cualificados, sellos electrónicos, sistemas de clave concertada y cualquier otro canal validado por el Estado.
- Firma de los interesados (Art. 10 Ley 39/2015): Requerida únicamente para formular solicitudes, presentar declaraciones responsables, interponer recursos, desistir de acciones y renunciar a derechos.
- Uso obligatorio de Cl@ve: Plataforma común para identificación y firma no criptográfica mediante Cl@ve PIN y Cl@ve Permanente.
- Actuación administrativa automatizada (Art. 41 Ley 40/2015): Actos sin intervención directa del funcionario, mediante sello electrónico de órgano o Código Seguro de Verificación (CSV).
- Firma del personal funcionario (Art. 43 Ley 40/2015): Uso obligatorio de firma electrónica cualificada vinculada a su puesto funcional, garantizando anonimato en casos protegidos.

Concepto / Dimensión	Identificación (Art. 9 LPACAP)	Firma Electrónica (Art. 10 LPACAP)
Finalidad legal	Acreditar la identidad del interesado ante la Administración Pública	Manifestar la voluntad, conformidad y autoría respecto a un contenido jurídico
Exigibilidad en el procedimiento	Obligatoria con carácter general para cualquier interacción o consulta	Tasada legalmente: formular solicitudes, recursos, renuncias y desistimientos
Mecanismos admitidos	Certificados cualificados, sellos, claves concertadas (Cl@ve) y registro previo	Firma electrónica avanzada/cualificada y sistemas Cl@ve Firma vinculados a certificado
Efecto en actuaciones automatizadas	Verificación de acceso a sede electrónica o portal	Generación de sello electrónico de Administración o CSV (Arts. 41-42 LRJSP)

> **Atención Opositor:** *Salvo precepto legal expreso, las Administraciones Públicas no pueden exigir un nivel de firma superior al mínimo estrictamente proporcional a los riesgos del trámite (Art. 10.4 LPACAP).*

5. Reglamento eIDAS (Reglamento UE 910/2014 y modificaciones del Reglamento UE 2024/1183)

Ámbito, objetivos y niveles de seguridad de la identificación electrónica

El Reglamento eIDAS establece un marco jurídico común para la identificación electrónica y los servicios de confianza en el mercado interior de la UE.

Garantiza el reconocimiento transfronterizo de los medios de identificación electrónica expedidos por los Estados miembros conforme a niveles de seguridad predeterminados.

- Nivel de seguridad bajo: se refiere a medios que ofrecen un grado limitado de confianza en la identidad declarada.
- Nivel de seguridad sustancial: exige controles para mitigar significativamente el riesgo de uso indebido o alteración.
- Nivel de seguridad alto: exige controles para impedir totalmente el uso indebido o la alteración (basado en hardware criptográfico, biometría o verificación estricta).
- Principio de reconocimiento mutuo: la Administración Pública debe admitir medios de nivel sustancial o alto expedidos por otros Estados si exige dicho nivel para sus propios servicios.

Nivel de Seguridad	Requisitos de Autenticación	Equivalencia en Esquema Nacional de Interoperabilidad / Seguridad
Bajo	Un solo factor (usuario y contraseña básica sin verificación reforzada)	Nivel Bajo (mínima repercusión si se vulnera)
Sustancial	Doble factor de autenticación (OTP, SMS seguro o software específico)	Nivel Medio (repercusión moderada)
Alto	Doble factor resistente a interceptación con soporte hardware o biométrico seguro	Nivel Alto (máxima repercusión y seguridad física)

> **Atención Opositor:** *El Reglamento (UE) 2024/1183 (eIDAS 2) introduce la Cartera Europea de Identidad Digital (European Digital Identity Wallet), que deberá suministrarse de forma obligatoria y gratuita para personas físicas.*

Servicios de confianza: tipología, efectos jurídicos y requisitos cualificados

Diferencia formalmente entre servicios de confianza estándar y servicios de confianza cualificados (que gozan de presunción legal de validez en toda la UE).

La firma electrónica y el sello electrónico comparten la misma jerarquía de niveles: simple, avanzada y cualificada.

- Firma electrónica cualificada: se crea mediante un dispositivo cualificado de creación de firmas (QSCD) y se basa en un certificado cualificado; equivale jurídicamente a una firma manuscrita.
- Sello electrónico: exclusivo para personas jurídicas para certificar el origen y la autenticidad de sus documentos.
- Sello de tiempo cualificado: goza de presunción de exactitud de la fecha y hora indicadas y de integridad de los datos asociados.
- Servicio de entrega electrónica certificada cualificado: presume la integridad de los datos, el envío, la recepción y la exactitud temporal.

- Organismo de supervisión en España: Ministerio para la Transformación Digital y de la Función Pública.

Figura Jurídica	Titular	Equivalencia Jurídica Principal	Dispositivo / Requisito Exigido
Firma Electrónica Cualificada	Persona física	Firma manuscrita (Art. 25.2 eIDAS)	QSCD + Certificado cualificado
Sello Electrónico Cualificado	Persona jurídica	Presunción de autenticidad e integridad del documento	Dispositivo seguro de creación de sellos + Certificado cualificado
Sello de Tiempo Cualificado	Proveedor de confianza	Presunción de exactitud temporal y no alteración	Fuente de tiempo vinculada a UTC + Firma/Sello cualificado

> **Atención Opositor:** *A una firma electrónica no se le pueden denegar efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales únicamente por estar en formato electrónico o no ser cualificada (Art. 25.1 eIDAS).*

6. El Documento Nacional de Identidad Electrónico (DNIe)

Marco normativo, naturaleza jurídica y certificados incorporados

El DNIe está regulado por la Ley Orgánica 4/2015 de Protección de la Seguridad Ciudadana, el Real Decreto 1553/2005 y la Ley 6/2020 de servicios electrónicos de confianza.

Acredita no solo la identidad física y la nacionalidad de su titular, sino también la identidad electrónica con valor de firma cualificada.

- Certificado de Autenticación: garantiza la identidad del ciudadano en medios telemáticos (firma electrónica avanzada para identificación).
- Certificado de Firma: genera firmas electrónicas cualificadas con el mismo valor legal que la firma manuscrita.
- Componente de hardware: chip criptográfico homologado como Dispositivo Cualificado de Creación de Firma (QSCD) bajo normas Common Criteria (nivel EAL5+ o superior).
- Clave privada: no sale nunca del chip criptográfico y su activación exige PIN o verificación biométrica.
- Validez temporal: el soporte físico dura 5 o 10 años (o permanente para mayores de 70 años), pero los certificados criptográficos caducan a los 5 años (o 2 años en versiones previas).

Versión del DNI	Interfaz de Comunicación	Nivel de Certificación	Características Principales
DNIe 3.0	Contacto y Contactless (NFC y Dual Interface)	CC EAL5+ / QSCD	Lectura rápida por NFC en smartphones y antenas RFID
DNIe 4.0 (DNI Europeo)	Contacto y Contactless	CC EAL6+ / QSCD /	Adaptación al

	(NFC optimizado)	eIDAS High	Reglamento (UE) 2019/1157, código de país en bandera UE y microchip ARM

> **Atención Opositor:** *El DNIe es clasificado dentro del marco eIDAS como medio de identificación electrónica de nivel de seguridad ALTO, siendo el máximo exponente de soberanía criptográfica en España.*

Ecosistema de uso: Autoridad de Certificación, ciclo de vida y DNI en el móvil

La Autoridad de Certificación emisora del DNIe es la Dirección General de la Policía (DGP), actuando como Prestador Cualificado de Servicios de Confianza.

La revocación y renovación del ciclo de vida de los certificados se gestiona mediante los Puntos de Actualización del DNIe (PAD) en comisarías o mecanismos remotos autorizados.

- Puntos de Actualización del DNIe (PAD): quioscos físicos que permiten renovar claves y certificados mediante lectura biométrica de la huella dactilar, sin cita previa.
- Revocación de certificados: automática ante denuncia por pérdida o sustracción, o por solicitud telemática validada.
- DNI en el móvil: iniciativa MiDNI enmarcada en el Reglamento UE 2024/1183 para permitir la acreditación de la identidad desde smartphones mediante credenciales verificables.
- Compatibilidad técnica: requiere lectores de tarjetas inteligentes compatibles con ISO 7816 o terminales NFC que soporten el protocolo PACE (Password Authenticated Connection Establishment).

> **Atención Opositor:** *La clave pública de los certificados del DNIe está contenida en el propio certificado X.509 v3, mientras que la clave privada está blindada dentro del chip y nunca puede ser extraída ni exportada.*

7. Claves para el Examen

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

Trampas habituales de los tribunales

- Firma electrónica vs Sello electrónico: el tribunal intercambia que el sello es para personas físicas y la firma para personas jurídicas (es exactamente al revés: la firma identifica personas físicas y el sello identifica personas jurídicas).
- No discriminación de la firma simple/avanzada: los tribunales suelen afirmar incorrectamente que una firma electrónica no cualificada carece de validez legal, vulnerando el Art. 25.1 eIDAS que prohíbe rechazarla exclusivamente por ser electrónica.
- Duración de la tarjeta física vs Certificados del DNIe: confunden el periodo de vigencia del soporte plástico del DNI (5 o 10 años) con la vigencia de los certificados criptográficos del chip (máximo 5 años).

- Reconocimiento transfronterizo: suelen indicar que un Estado miembro está obligado a admitir medios de nivel bajo de otros países, cuando la obligación rige únicamente para niveles sustancial o alto (Art. 6 eIDAS).

Plazos críticos de obligada memorización

- Validez de los certificados del DNIe: actualmente tienen una vigencia máxima de 5 años desde su expedición o renovación.
- Validez del soporte DNI físico: 2 años para menores de 5 años, 5 años para menores de 30 años, 10 años entre 30 y 70 años, y permanente a partir de los 70 años o con gran invalidez.
- Notificación de brechas de seguridad por prestadores de confianza cualificados: deberán notificar al organismo de supervisión en un plazo máximo de 24 horas tras tener constancia del incidente (Art. 19.2 eIDAS).
- Conservación de información por prestadores cualificados (Ley 6/2020): deben conservar la información relativa a servicios prestados durante 15 años tras el cese de los efectos del servicio.

Artículos clave y preguntas frecuentes

- Artículo 25 Reglamento eIDAS: Efectos jurídicos de las firmas electrónicas (apartado 1: admisibilidad de no cualificadas; apartado 2: equivalencia cualificada con firma manuscrita).
- Artículo 26 Reglamento eIDAS: Requisitos intrínsecos de la firma electrónica avanzada (vinculada al firmante de manera única, permitir su identificación, creada con datos bajo su control exclusivo y vinculada a los datos de forma que cualquier cambio ulterior sea detectable).
- Artículo 35 Reglamento eIDAS: Efectos jurídicos de los sellos electrónicos (presunción de integridad y exactitud del origen para sellos cualificados).
- Artículo 9 y 10 Ley 39/2015: Sistemas de identificación y de firma admitidos por las Administraciones Públicas, remitiéndose expresamente a eIDAS.

Distinciones conceptuales finas

- Firma Electrónica Avanzada vs Firma Electrónica Cualificada: la avanzada cumple los requisitos del art. 26; la cualificada es una avanzada que además se crea con un dispositivo cualificado (QSCD) y se basa en un certificado cualificado expedido por un prestador cualificado.
- Prestador de Servicios de Confianza vs Prestador CUALIFICADO: cualquiera puede prestar servicios de confianza, pero solo el cualificado pasa auditoría previa de conformidad, figura en la Lista de Confianza (TSL) y sus emisiones gozan de presunción legal iuris tantum.
- PACE vs BAC en DNIe: BAC (Basic Access Control) permitía lectura por MRZ básica; PACE (Password Authenticated Connection Establishment) es el protocolo criptográfico robusto obligatorio desde DNIe 3.0 para acceso inalámbrico NFC.
- Certificado de Autenticación vs Certificado de Firma del DNIe: el de autenticación no sirve para rubricar contratos o trámites formales equivalentes a manuscrito, solo para iniciar

sesión cifrada o handshake TLS/SSL; la manifestación de voluntad exige el certificado de firma.

8. Cuadro Resumen Esquemático

Concepto / Epígrafe	Fundamento Legal (Art. y Ley)	Elementos Clave / Plazos / Mayorías	Clave para Examen
Reglamento eIDAS (Identificación)	Reglamento (UE) 910/2014, Arts. 6-12	Niveles de seguridad: Bajo, Sustancial y Alto. Obligación de admisión para nivel sustancial y alto.	Solo los niveles sustancial y alto gozan de reconocimiento transfronterizo obligatorio en AAPP.
Firma y Sello Electrónico	Reglamento (UE) 910/2014, Arts. 25-35	Firma para personas físicas; sello para personas jurídicas. Tres niveles: simple, avanzada y cualificada.	Solo la firma cualificada equivale ex lege a la firma manuscrita tradicional (Art. 25.2).
Servicios de Confianza y Supervisión	Ley 6/2020 y eIDAS Arts. 17-24	Conservación de registros durante 15 años. Notificación de brechas de seguridad en 24 horas.	El órgano supervisor en España es el Ministerio para la Transformación Digital y de la Función Pública.
Documento Nacional de Identidad Electrónico	RD 1553/2005 y LO 4/2015	2 certificados en chip (Autenticación y Firma). Certificados caducan a los 5 años; soporte físico entre 5 y 10 años.	Chip catalogado como QSCD; proporciona nivel de seguridad ALTO en el marco eIDAS.
Identificación y Firma en el Procedimiento	Ley 39/2015, Arts. 9-11	Diferenciación estricta entre identificación (acreditar quién es) y firma (manifestar voluntad o consentir).	Para formular solicitudes o desistir es preceptiva la firma; para la mera consulta basta la identificación.