Mapa regulatorio de Ciberseguridad en la UE

El presente compendio ofrece una visión estructurada del marco regulatorio europeo en materia de ciberseguridad, datos, servicios digitales e identidad electrónica. Reúne de forma sintética los objetivos, obligaciones y elementos esenciales de cada normativa para facilitar su comprensión operativa y su impacto real en las organizaciones.

Índice

1. Introducción

La Unión Europea ha impulsado durante los últimos años un marco común de ciberseguridad destinado a reforzar la protección de infraestructuras, servicios esenciales y ecosistemas digitales frente a amenazas crecientes y más sofisticadas. Este marco se ha ido ampliando en respuesta a evoluciones tecnológicas y geopolíticas que exigen una mayor coordinación europea, dando lugar a un entramado normativo que incluye reglamentos de aplicación directa, directivas sujetas a transposición nacional y estándares internacionales voluntarios.

Sin embargo, este entramado regulatorio se ha convertido en un ecosistema complejo y poco integrado, donde distintas iniciativas conviven con diferencias de enfoque y obligaciones que no siempre encajan de forma armónica. La coexistencia de múltiples instrumentos con ámbitos distintos — algunos horizontales, otros sectoriales— genera desafíos de interpretación y aplicación coherente.

Esta guía nace precisamente para responder a esa necesidad: ofrecer una visión comprensible y operativa que permita a cualquier organización situarse dentro de este entramado regulatorio sin necesidad de ser experta en derecho, en ciberseguridad o en políticas digitales. Su objetivo es doble: primero, ayudar a identificar qué normas aplican a cada caso; y segundo, traducir esas normas en implicaciones reales y accionables para el día a día de la organización.

La guía está dirigida a responsables de cumplimiento normativo, asesores jurídicos, directivos y equipos técnicos de organizaciones que operan en la Unión Europea o prestan servicios a entidades europeas. No se requieren conocimientos jurídicos especializados para su utilización: el contenido se ha redactado con un enfoque práctico y accesible.

2. Funcionamiento de la Guía

El marco regulatorio europeo en materia de ciberseguridad, datos y entorno digital no responde a una única norma, sino a un conjunto de disposiciones de distinta naturaleza y alcance que se superponen e interactúan entre sí.

Con el objetivo de facilitar su comprensión, la guía se ha diseñado siguiendo un enfoque visual y estructurado, que permite entender el conjunto normativo como un sistema coherente y no como una suma aislada de reglas.

Esta lógica se representa gráficamente mediante la diana normativa, que muestra el marco regulatorio como un sistema de anillos concéntricos. En el centro se sitúan las normas más estructurales y transversales, mientras que en los anillos exteriores aparecen aquellas que se activan en función del sector, del tipo de servicio prestado o de tecnologías concretas. De este modo, la diana ayuda a visualizar que no todas las organizaciones están sujetas a todas las normas, sino que se van integrando. Se recomienda consultar la leyenda incluida junto al gráfico para identificar la correspondencia entre colores, iconos y bloques normativos.

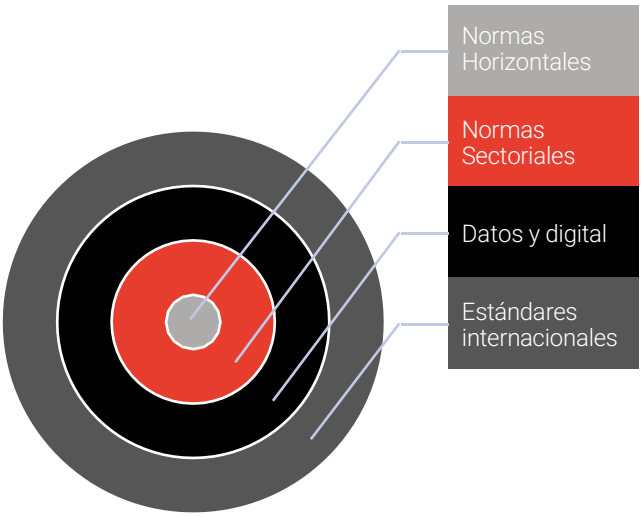
Este sistema de etiquetado y clasificación permite situar cada instrumento normativo dentro del siguiente marco conceptual descrito:

- En el primer anillo se sitúan aquellas normas que actúan como la columna vertebral: fijan los mínimos obligatorios de seguridad, resiliencia y certificación que toda organización debe demostrar.

- En el segundo anillo se localizan las normas sectoriales (como DORA o el European Health Data Space) que ajustan el marco, reforzando el cumplimiento normativo en los sectores específicos donde una afectación puede desencadenar efectos en cadena: finanzas, energía, infraestructuras críticas.

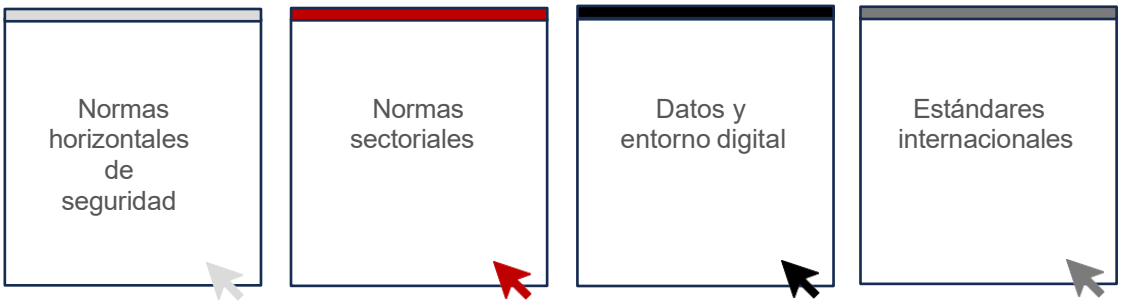
- En el tercer anillo se integra el bloque datos y digital con las normas que regulan todo lo que mueve el mundo digital moderno: datos personales, identidades, plataformas, algoritmos, inteligencia artificial y competencia.

- En el cuarto anillo se desarrollan los estándares internacionales más relevantes para la ciberseguridad.



En este sentido, la guía clasifica cada norma dentro de uno de los siguientes bloques temáticos: (i) normas horizontales de ciberseguridad, (ii) normas sectoriales, (iii) regulación de datos y entorno digital, y (iv) estándares internacionales.

Así, cada normativa se asocia a una etiqueta, color e iconos concretos que indican el nivel —horizontal, sectorial, datos y digital o estándares internacionales— al que pertenece. Los anillos funcionan como bloques temáticos que se identifican con una forma geométrica y un color distinto.



La guía desarrolla cada una de las normas que se integran en estos bloques en forma de fichas normativas. Cada ficha normativa sigue una estructura uniforme que incluye los siguientes apartados:

- # Base normativa
- # Objetivo
- # Aplicación temporal
- # Sujetos obligados
- # Obligaciones principales
- # Régimen sancionador

Esta estandarización permite comparar rápidamente las distintas normas y localizar la información relevante de forma inmediata.

NIS2

Norma sujeta a transposición que regula la ciberseguridad para medianas o grandes empresas de sectores críticos en la UE.

NIS2

Directiva (UE) 2022/2555 (“NIS2”) del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión y por la que se deroga la Directiva (UE) 2016/1148 (“NIS”).

Garantizar un nivel elevado, homogéneo y resiliente de ciberseguridad en la Unión Europea, reforzando la capacidad de respuesta frente a amenazas y aumentando la protección de los sectores críticos.

17 octubre 2024, límite transposición. España aprobó el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, pendiente de tramitación parlamentaria.

Empresas y entidades públicas o privadas de los sectores esenciales (**Anexo I**: energía, transporte, banca, infraestructuras de mercados financieros, salud, agua potable, aguas residuales, infraestructura digital, gestión de servicios TIC B2B, sector espacial, administración pública) e importantes (**Anexo II**: servicios postales, gestión de residuos, fabricación, proveedores digitales, investigación, alimentación, industria química).

- Cuando sean medianas o grandes empresas (≥50 empleados o ≥10M€ facturación)

- Implantar un Sistema de Gestión de riesgos de ciberseguridad (artículo 21)

- Notificación de incidentes significativos (alerta temprana en 24h, notificación en 72h, informe final en un mes)

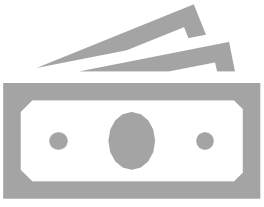
- Seguridad en la cadena de suministro TIC

- Gobernanza y responsabilidad de la dirección
- Documentación, trazabilidad y supervisión.

Económicas máximas:

- Entidades esenciales: hasta 10 M€ o 2% del volumen de negocio anual

- Entidades importantes: hasta 7 M€ o 1,4% del volumen de negocio anual



EU Cybersecurity Act

Reglamento que establece el marco europeo de certificación de ciberseguridad para fabricantes y proveedores TIC.

EU CYBERSECURITY ACT (CSA)

Reglamento (UE) 2019/881, de 17 de abril de 2019, relativo a ENISA y al marco europeo de certificación de ciberseguridad para productos, servicios y procesos TIC.

Reforzar el mandato permanente de ENISA y crear un marco europeo común de certificación de ciberseguridad que garantice un nivel adecuado de confianza en productos, servicios y procesos TIC dentro del mercado único digital.

Aplica directamente en todos los Estados miembros desde el 27 de junio de 2019.

No impone obligaciones directas a empresas, sino que establece un marco voluntario de certificación (que puede devenir obligatorio cuando otras normas lo exijan)

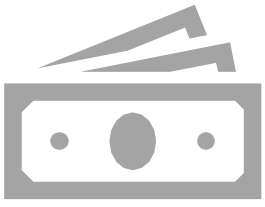
Pueden certificarse: (i) empresas y organizaciones que diseñen, produzcan, integren o comercialicen productos, servicios o procesos TIC en la UE, (ii) presten servicios digitales o gestionen infraestructuras TIC relevantes y/o (iii) sean fabricantes de hardware, software o dispositivos conectados.

Cumplir los esquemas europeos de certificación aplicables y emitir la declaración UE de conformidad.

- Conservar la documentación técnica del producto certificado.

- Notificar vulnerabilidades y disponer de política de divulgación coordinada.

- Retirada, suspensión o no reconocimiento del certificado europeo.
- Prohibición temporal de comercialización de productos o servicios no conformes.
- Exclusión de licitaciones públicas cuando certificación exigible.
- Pérdida de confianza y riesgos operativos derivados de productos inseguros.



Cyber Resilience Act

Reglamento que obliga a los fabricantes, importadores, distribuidores y proveedores de productos de software o hardware con elementos digitales, comercializados en la UE, a que sean seguros por diseño y mantengan soporte de seguridad durante su vida útil.

CYBER RESILIENCE ACT (CRA)

Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales.

Establecer un marco armonizado y obligatorio para que todos los elementos digitales en la UE garanticen la ciberseguridad y reduzca las vulnerabilidades desde el diseño.

Entrada en vigor en 2024, aplicación principal a partir del 11 de diciembre de 2027 y obligaciones concretas:

Artículo 14: desde el 11 de septiembre de 2026. Capítulo IV (arts. 35 a 51): desde el 11 de junio de 2026.

Fabricantes, importadores y distribuidores de productos digitales, de cualquier tamaño, dirigidos tanto a consumo de particulares como empresariales.

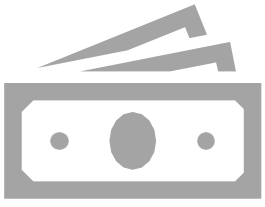
- Diseñar productos digitales con requisitos esenciales de ciberseguridad desde el diseño y por defecto (Anexo I).

-Evaluación de conformidad, declaración UE de conformidad, marcado CE, y obligación de actualizaciones de seguridad continua durante el ciclo de vida del producto.

-Documentación: evaluación riesgos, documentación técnica (Anexo VII).

Sanciones económicas

- Hasta 15 millones de euros, o 2,5% del volumen de negocio total anual, si fuese superior.
- Hasta 10 millones de euros, o 2% del volumen de negocio total anual, si fuese superior.
- Hasta 5 millones de euros, o 1% del volumen de negocio total anual, si fuese superior.



CER Directive

Directiva que refuerza la resiliencia física y operativa de entidades crítica que prestan servicios esenciales frente a amenazas naturales, técnicas o intencionadas.

CER DIRECTIVE

Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.

Establecer un marco común en la UE centrado en garantizar la resiliencia frente a amenazas no cibernéticas (físicas, naturales, humanas) que se integra con NIS2, garantizando coherencia entre la resiliencia física y la seguridad digital para asegurar la prestación ininterrumpida de servicios esenciales.

Aplicable desde 18 de octubre de 2024. Aprobado el Proyecto de Ley y Resiliencia de Entidades Críticas ("LPREC") para su transposición en España.

Entidades críticas identificadas por los Estados miembros:

- Energía; Transporte; Banca; Infraestructuras de mercados financieros; Sanidad; Agua potable; Aguas residuales; Infraestructura digital; Administración Pública; Espacio y Producción y distribución alimentaria.

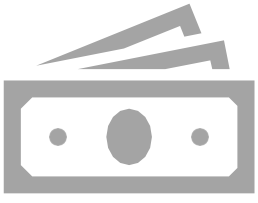
Se excluyen entidades cuya actividad principal sea defensa, seguridad nacional, seguridad pública o fuerzas de seguridad.

Debe realizarse una evaluación de riesgos en ≤9 meses tras la notificación de designación como entidad crítica y al menos cada 4 años.

Se deberá designar un punto de contacto.

Incluye obligación de notificación de incidentes físicos/operativos: inicial ≤24h e informe detallado ≤1 mes.

Los Estados Miembros deben establecer un régimen sancionador propio (art. 22).



Esquema Nacional de Seguridad (ENS)

Marco obligatorio de seguridad para administraciones públicas españolas y proveedores que gestionan sistemas o servicios públicos

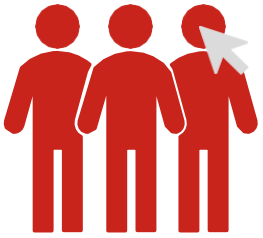
ENS ESQUEMA NACIONAL DE SEGURIDAD

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Establecer los principios básicos y requisitos mínimos que aseguran la protección adecuada de la información y servicios electrónicos del sector público español..

En vigor desde el 5 de mayo de 2022.

- Todo el sector público español.
- Sistemas que traten información clasificada.
- Entidades privadas que presten servicios al sector público español.
- Sistemas relacionados con redes y servicios 5G.



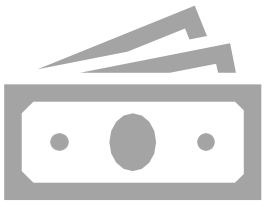
Categorización del sistema en tres categorías de seguridad (BÁSICA, MEDIA, ALTA) y medidas de gobernanza, gestión del riesgo, continuidad y resiliencia modulables en función de dicha categorización.

Proceso de certificación de conformidad con el ENS.

ENS no tiene régimen sancionador autónomo, pero los efectos del incumplimiento son:

Suspensión del servicio.

Responsabilidad disciplinaria sobre personal interno.



Reglamento Delegado (UE) 2022/30

Norma que introduce requisitos obligatorios de ciberseguridad, protección de datos y prevención del fraude para los equipos radioeléctricos comercializados en la UE.

REGLAMENTO 2022/30

Reglamento Delegado (UE) 2022/30 de la Comisión, de 29 de octubre de 2021,que completa la Directiva 2014/53/UE (Radio Equipment Directive – RED) en relación con los requisitos esenciales de ciberseguridad, protección de datos personales, privacidad y protección contra el fraude.

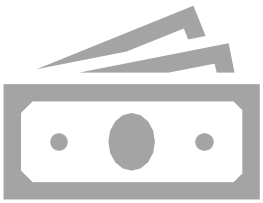
Reforzar la ciberseguridad y la protección de las personas garantizando que determinados equipos radioeléctricos introducidos en el mercado de la UE no perjudiquen a las redes, protejan los datos personales y la privacidad, y prevengan el fraude cuando ejecutan funciones sensibles.

Aplicación obligatoria: 1 agosto 2025.

Agentes económicos que fabriquen, importen o comercialicen equipos radioeléctricos en la UE.

- Evitar prácticas que dañen o degraden sistemas de información ni redes.
- Los equipos capaces de tratar datos personales, de tráfico o localización deben incorporar salvaguardas técnicas.
- Los equipos que permitan pagos deben incluir mecanismos que reduzcan el riesgo de fraude.

- Prohibición de comercialización o retirada del mercado.
- Responsabilidad civil.



DORA

Reglamento que unifica la resiliencia operativa digital para entidades financieras y proveedores TIC críticos.

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero (DORA)

Garantizar un nivel elevado, uniforme e integral de resiliencia operativa digital en todo el sector financiero de la UE, con aplicación de lex specialis respecto de NIS2.

Entrada en vigor: 16 enero 2023; Aplicación obligatoria 17 enero 2025.

21 categorías de entidades financieras (art. 2), incluyendo entidades de crédito, empresas de inversión, entidades de pago, entidades de dinero electrónico, etc.

También los proveedores terceros de servicios TIC que presten servicios a dichas entidades.

- Implementar un Sistema de Gestión del riesgo TIC.

-Notificación de incidentes en plazos de 4 horas (graves), 24 horas (informe inicial), 72 horas (informe intermediario) y final (30 días).

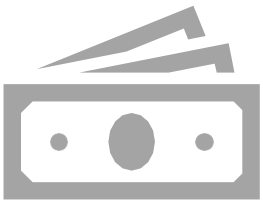
-Pruebas periódicas de resiliencia (incl. TLPT cada 3 años para entidades significativas)

-Contratos con proveedores TIC que incorporen las cláusulas de los artículos 30.2 y 30.3.

Sanciones administrativas, requerimientos, limitaciones o prohibiciones operativas. A determinar por cada Estado miembro.

Para proveedores TIC críticos sujetos al marco de supervisión directa:

- Multas coercitivas (hasta un 1% del volumen de negocios diario durante un máximo de 6 meses).
- Obligación de modificar contratos y medidas técnicas.



Directiva 2015/2366 (PSD2)

Directiva que regula los servicios de pago de la UE para aumentar la seguridad, fomentar la competencia y

Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior, conocida como PSD2 (Payment Services Directive 2), y por la que se deroga la Directiva 2007/64/CE (PSD1).

Crear un mercado único de pagos más seguro, competitivo e innovador en la UE, reforzando la protección del usuario, fomentando la competencia (open banking) y reduciendo el fraude en pagos electrónicos.

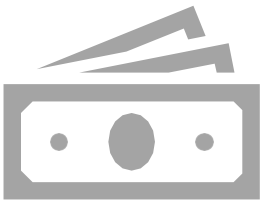
Aplicable tras su transposición nacional (13 de enero de 2018), incorporada en España mediante el Real Decreto-ley 19/2018.

Proveedores de servicios de pago (PSP) de entre los comprendidos en el Anexo I.

Obliga en particular a aplicar autenticación reforzada del cliente (SCA) en los servicios de pago. A su vez, introduce el marco de *open banking*, garantizando al mismo tiempo una gestión activa de los riesgos operativos y de seguridad, así como la protección de datos del cliente y la prevención del fraude.

No sustituye las obligaciones de DORA, sino que se complementan.

- Sanciones administrativas impuestas por el Banco de España.
- Suspensión o revocación de la autorización como proveedor de servicios de pago



European Health Data Space (EHDS)

Marco europeo común para el acceso, intercambio y reutilización segura de los datos de salud electrónicos.

EHDS

Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud

Crear un marco europeo común para el acceso, intercambio y reutilización segura de los datos de salud electrónicos.

Entrada en vigor: 25 de marzo de 2025.

-Organizaciones públicas y privadas del ámbito sanitario y tecnológico.

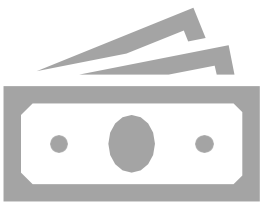
Medidas orientadas a garantizar el acceso inmediato a los datos de salud. A su vez, busca asegurar su interoperabilidad mediante el formato europeo de historia clínica electrónica.

Se refuerza la gobernanza del dato sanitario para evitar su reidentificación.

Regula el uso secundario solo para fines lícitos de investigación, salud pública e innovación. Todo en coordinación con el RGPD.

- Multas administrativas alineadas con el RGPD.
- Responsabilidad civil por daños a interesados.
- Exclusión temporal o definitiva del acceso al EHDS.

La reidentificación de datos se considera infracción grave.



Reglamento General de Protección de Datos (RGPD)

Reglamento que protege los datos personales de cualquier ciudadano de la UE.

RGPD

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE.

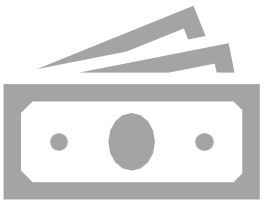
Proteger los derechos y libertades fundamentales de las personas garantizando su derecho a la protección de datos personales y regular la libre circulación de tales datos.

Aplicación obligatoria: 25 mayo 2018.

- Responsables y encargados del tratamiento
- Organizaciones fuera de la UE que traten datos personales de interesados que se encuentren en la UE cuando: (i) ofrezcan bienes o servicios a interesados en la UE y (ii) monitorización de comportamiento dentro UE.

Tratar los datos de forma licíta, de acuerdo con las bases de legitimación (art. 6) y los principios del RGPD. Se obliga a designar un DPO, en determinados supuestos, así como a llevar un registro de actividades de tratamiento, realizar evaluaciones de impacto y notificar a la AEPD las brechas de datos en 72 horas así como a los interesados cuando el riesgo sea elevado.

Hasta 10.000.000 € o el 2 % del volumen de negocio anual global en los supuestos menos graves,
hasta 20.000.000 € o el 4 % del volumen de negocio anual global en los más graves, aplicándose siempre la cifra de mayor cuantía.



Data Act

Reglamento que garantiza el acceso, uso y portabilidad de los datos generados por fabricantes, proveedores de servicios conectados, receptores de datos y proveedores cloud.

DATA ACT

Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización.

Establecer un marco horizontal para garantizar un acceso justo, seguro y regulado a los datos, personales y no personales, generados por productos conectados y servicios digitales asociados (IoT), que remite al RGPD cuando se trata de datos personales, si bien con prevalencia de este último.

Entrada en vigor: 11 de enero de 2024 Aplicación: 12 septiembre 2025.

Empresas obligadas:

- Fabricantes de productos conectados; Proveedores de servicios relacionados; Titulares y destinatarios de datos; Proveedores de servicios cloud; Desarrolladores de contratos inteligentes para compartir datos y Participantes en espacios comunes europeos de datos

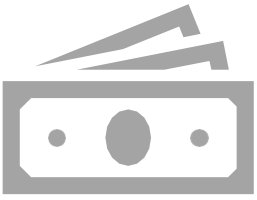
Exenciones Micro y pequeñas empresas como fabricantes de productos conectados (salvo que estén asociadas a grandes empresas).

Obliga a diseñar productos y servicios que permitan que los datos (y metadatos, en su caso) sean accesibles por diseño y por defecto. Se regula un acceso público excepcional en emergencias; interoperabilidad e intercambio automatizado (APIs/estándares).

Se establecen controles técnicos por medio de auditorías de seguridad y cifrado.

Se deben documentar políticas de acceso, contratos cloud conformes y registros de solicitudes.

Cada Estado miembro debe aprobar sus propias reglas sobre sanciones por incumplimiento, y que esas sanciones deben ser efectivas, proporcionadas y disuasorias.



eIDAS2

Reglamento que crea la Identidad Digital Europea para identificarse y firmar electrónicamente en toda la UE.

eIDAS 2

Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo relativo al establecimiento del marco europeo de identidad digital.

Crear un Marco Europeo de Identidad Digital interoperable que permita a cualquiera usar una Cartera Europea de Identidad Digital para identificarse, firmar y gestionar atributos en toda la UE.

Aplicable desde 20 de mayo de 2024. Los Estados miembros deben implementar las carteras antes de noviembre de 2026.

- Estados Miembros de la UE.
- Sector público y sector privado para sectores que requieran autenticación reforzada en bancos y servicios financieros, sanidad, transporte, energía, telecomunicaciones, servicios digitales críticos y grandes plataformas.
- Prestadores de servicios de confianza (cualificados y no cualificados).
- Empresas que actúan como partes usuarias.

Se debe ofrecer la Cartera EUDI por parte de los Estados Miembros.

- Proveedores de Cartera: código abierto, seguridad desde el diseño, separación lógica, control del usuario, portabilidad, firma cualificada gratuita y notificación de brechas.
- Partes usuarias: registro previo, minimización de datos y aceptación de seudónimos cuando la ley lo permita.
- Prestadores de confianza: auditorías, notificación en 24 horas, verificación de identidad y gestión de riesgos.

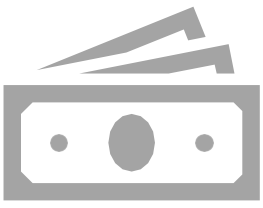
Estados Miembros establecerán, con máximos de hasta 5.000.000€ o ;1% del volumen de negocio total anual, si fuese superior.

Impactos legales:

Retirada de la cualificación de servicios de confianza.

Suspensión o cese de la cartera digital.

Responsabilidad por daños.



ePrivacy

Norma dirigida a los proveedores de servicios electrónicos que protege la confidencialidad de las comunicaciones electrónicas, regula cookies, datos de localización y marketing digital.

ePrivacy

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Garantizar la confidencialidad de las comunicaciones electrónicas y la protección de la información.

En vigor desde 31 de julio de 2002. Transposición española: LSSI (Ley 34/2002) y LGT (Ley 9/2014) en lo que corresponde.

- Sector público y privado.
- Usuarios finales, abonados y cualquier persona física o jurídica cuyas comunicaciones electrónicas pueden ser afectadas.

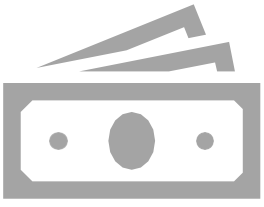
Obligaciones de garantizar la confidencialidad de las comunicaciones electrónicas y seguridad de redes.

Se requiere solicitar consentimiento previo para acceso a cookies (salvo técnicas o estrictamente necesarias) y evidencias de consentimiento.

Se deben establecer mecanismos de oposición al marketing.

Multas por envío de spam: hasta 150.000€.

Sanciones por incumplimientos de privacidad: hasta 20 millones de euros, o 4% del volumen de negocio total anual (cuando aplique RGPD).



IA Act

Reglamento que establece obligaciones estrictas y documentación obligatoria para garantizar un uso seguro, trazable y supervisado de los sistemas de Inteligencia Artificial en función de su nivel de impacto.

IA ACT

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, que establece normas armonizadas en materia de inteligencia artificial. El proyecto de reforma Ómnibus modifica sustancialmente el calendario de aplicación.

Marco común europeo que reduzca los riesgos derivados de sistemas de IA opacos, discriminatorios o inseguros.

Aplicabilidad general: 2 de agosto de 2026.

2 febrero 2025: prohibiciones y alfabetización IA.

02 de agosto de 2026 - información sobre interacción con IA; sanciones del RIA

02 de diciembre de 2026 - transparencia y marcado de contenidos; implementación de medidas de control de aplicaciones "nudifier"

02 de diciembre de 2027 - sistemas de IAs de alto riesgo autónomos

02 de agosto de 2028 - sistemas de alto riesgo que sean componentes de seguridad de productos regulados

- Proveedores/desarrolladores de IA.
- Importadores y distribuidores que comercialicen IA en la UE.
- Usuarios o desplegadores (deployers) de IA en actividades privadas o públicas.
- Proveedores de modelos de IA de propósito general (GPAI).

Se debe clasificar cada sistema de IA por riesgo (prohibido, alto o limitado) y aplicar las obligaciones correspondientes.

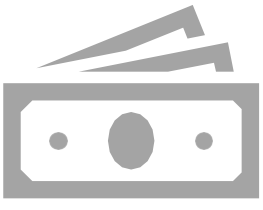
Establece medidas reforzadas para sistemas de alto riesgo, como pruebas de seguridad, documentación técnica detallada y procedimientos de auditoría.

Marcado CE como distintivo obligatorio.

Notificación de incidentes graves en 24 horas.

Hasta 35 millones € o 7% del volumen de negocio global (la cifra mayor).

Sanciones menores para incumplimientos de transparencia.



Digital Services Act (DSA)

Reglamento que establece obligaciones de diligencia para plataformas, intermediarios y buscadores, para garantizar un entorno online seguro.

DIGITAL SERVICES ACT (DSA)

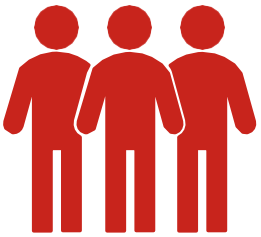
Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE

Crear un entorno digital seguro, predecible y fiable que proteja los derechos fundamentales para gestionar contenidos ilícitos y prácticas abusivas en línea.

Aplicable desde 17 febrero 2024.

A todos los prestadores de servicios intermediarios, con independencia de su tamaño o del país en el que estén establecidos, si ofrecen servicios dentro de la UE.

Ámbito territorial: Aplica también a empresas extracomunitarias con “conexión sustancial” con la UE.



Establecimiento de mecanismos claros de contacto y designación de representante en la UE cuando proceda.

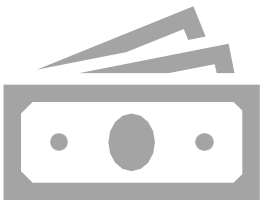
Gestión de contenidos ilícitos mediante procedimientos de *notice and action*, deber diligencia y derechos de reclamación de los usuarios.

Transparencia publicitaria y prohibición de dark patterns.

Para plataformas y buscadores de muy gran tamaño (VLOPs/VLOSEs): evaluación anual de riesgos, auditorías independientes, acceso a investigadores, repositorio público de anuncios y protocolo de crisis.

Hasta el 6% del volumen de negocio global anual: infracciones graves.

Hasta el 1% por información falsa o incompleta a autoridades.



Digital Markets Act (DMA)

Reglamento que limita prácticas abusivas de las grandes plataformas para garantizar mercados digitales contestables.

DIGITAL MARKETS ACT (DMA)

Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital.

Asegurar mercados digitales justos, evitando prácticas que distorsionen la competencia y los abusos de poder por parte de los gatekeepers...

Aplicable desde el 2 de mayo de 2023.

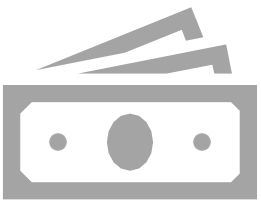
A. Gatekeepers. 3 requisitos:
1. Impacto significativo en el mercado
1.1. ≥ 7.500 M€ de facturación anual en UE en los últimos 3 años, o
1.2.≥ 75.000 M€ de capitalización.
1.3. Prestación del mismo servicio en ≥ 3 Estados miembros.
2. Importante puerta de acceso para usuarios profesionales hacia usuarios finales.
2.1. . ≥ 45 millones de usuarios finales activos/mes en la UE
2.1.2. ≥ 10.000 usuarios profesionales/año
3. Posición afianzada y duradera.
B. Servicios básicos de plataforma

Garantizar la interoperabilidad y apertura funcional de la plataforma, permitiendo el acceso a datos por usuarios profesionales y ofreciendo portabilidad en tiempo real para usuarios finales.

Prohibición de favorecer indebidamente los propios servicios del *gatekeeper* frente a los terceros.

Interoperabilidad de mensajería, tiendas/apps de terceros y elección por defecto.

Hasta el 10% del volumen de negocio mundial, y hasta 20% reincidencia.



ISO 27001

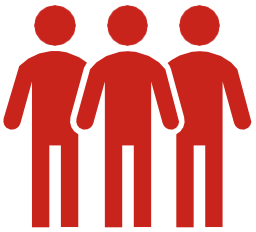
Estándar internacional para implantar un Sistema de Gestión de Seguridad de la Información basado en riesgos.

ISO 27001 - Sistema de Gestión de Seguridad de la Información

Establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información que proteja la confidencialidad, integridad y disponibilidad mediante un enfoque basado en riesgos.

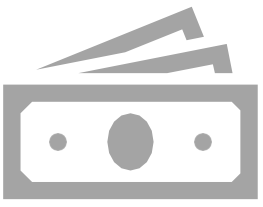
Última versión publicada el 25 de octubre de 2022

Organizaciones de cualquier tamaño o sector que gestionen información y activos críticos, presten servicios esenciales o tecnológicos, deban acreditar cumplimiento o busquen certificar su SGSI.



Implantar y mantener continuamente un SGSI basado en riesgos.

N/A



ISO 42001

Estándar internacional para gestionar el uso responsable y gobernado de la Inteligencia Artificial, que afecta a organizaciones que desarrollan, integran o utilizan IA y buscan implantar un marco de seguridad.

ISO/IEC 42001:2023 – Inteligencia Artificial

Implantar un sistema de gestión de IA que garantice un desarrollo y uso responsable, seguro y ético, gestione los riesgos algorítmicos y alinee la IA con la gobernanza, los derechos fundamentales y la regulación.

Publicada en diciembre de 2023.

Empresas, plataformas y entidades que desarrollan, integran o utilizan sistemas de IA, incluida la IA incorporada en servicios SaaS.

Establecer y revisar continuamente un sistema de gestión de IA responsable basado en riesgos.

N/A

ISO 27701

Estándar internacional para gestionar y demostrar la protección de la privacidad dentro de un sistema de gestión de seguridad de la información, para organizaciones que tratan datos personales.

ISO/IEC 27701:2025 – Seguridad de la información, ciberseguridad y protección de la

privacidad

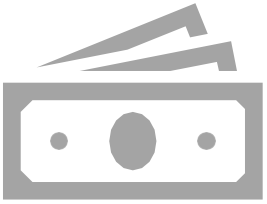
Marco estandarizado de gestión para que las organizaciones puedan establecer, implementar, mantener y mejorar un Sistema de Gestión de la Información sobre Privacidad.

Publicada en octubre de 2025.

Cualquier tipo de organización, especialmente para entidades que ya tienen ISO/IEC 27001 o, quieren demostrar madurez y gobernanza en privacidad.

Implementar y revisar continuamente un sistema de gestión de privacidad (PIMS).

N/A



9 NORMATIVAS CLAVE

¿Qué me aplica? *#ciberseguridad*

01 NIS2
Sectores esenciales e importantes

02 DATA ACT
Datos industriales, IoT y cloud

03 EHDS
Sector sanitario

04 RGPD
Datos personales

05 IA ACT
Sistemas de inteligencia artificial

06 CYBER RESILIENCE ACT (CRA)
Fabricantes de productos digitales

07 DIGITAL OPERATIONAL RESILIENCE ACT (DORA)
Sector financiero y proveedores

08 CER DIRECTIVE
Seguridad de entidades críticas

09 ENS (Esquema Nacional de Seguridad)
Sector público y proveedores

Desde ECIJA, quedamos a vuestra disposición ante cualquier consulta relacionada con esta materia.

ECIJA