Mapa de

Cybercompliance en seguridad de la información

dpi
DATA PRIVACY INSTITUTE

isms forum

csc
CYBER SECURITY CENTRE

Coordinadores

David Ferrete
Lyda Patiño
Raquel de Saá

Expertos participantes

Antonio Narbona
Agostina Lambertucci
Diego Fernández Vázquez
Francisco Rodríguez Valiente
Francisco Javier Carbayo
Ignacio Hornes Amenedo
José Luis García
Leocadio Marrero
María Ramírez
Marta Cañas
Manuel Estevez Ruiz
Miguel González-Santander
Sara Saceda
Beatriz García

Diseño y maquetación

Susana Marín

Índice

Prólogo

La **Seguridad de la Información** se ha consolidado como un pilar estratégico para la continuidad y resiliencia de las organizaciones. En el contexto actual, marcado por la transformación digital, la proliferación de ciberamenazas y la creciente dependencia tecnológica, la protección de la información ya no es únicamente una cuestión técnica: **es un imperativo normativo y de gobernanza corporativa.** Las Administraciones Públicas, tanto a nivel nacional como supranacional, han establecido marcos regulatorios cada vez más exigentes, reconociendo la seguridad como un elemento crítico para la estabilidad económica, la protección de derechos fundamentales y la confianza en los servicios digitales.

En este escenario, las organizaciones se enfrentan a un reto complejo: **identificar, interpretar y cumplir un entramado normativo en constante evolución.** La diversidad de regulaciones, estándares y directrices aplicables exige un enfoque sistemático que permita integrar el cumplimiento normativo en la gestión de riesgos y en la planificación estratégica de la ciberseguridad. Este ejercicio no solo es necesario para evitar sanciones, sino también para garantizar la resiliencia operativa y organizacional, así como la reputación corporativa.

Con el Mapa de Cybercompliance en Seguridad de la Información, desde ISMS Forum hemos querido sentar las bases para facilitar este análisis. Nuestro objetivo es proporcionar a las organizaciones una herramienta práctica que les permita:

- **Identificar las normativas y estándares aplicables a su actividad.**
- **Comprender las obligaciones específicas en materia de seguridad de la información.**
- **Incorporar estos requisitos en sus planes directores de ciberseguridad y en sus modelos de gestión de riesgos.**

Para ello, hemos elaborado un **mapa normativo inicial**, acompañado de fichas descriptivas que incluyen:

— **Resumen ejecutivo** de cada normativa.
— **Ámbito de aplicación** y criterios para determinar su aplicabilidad.
— **Elementos clave**, como la existencia de autoridades de control, regímenes sancionadores y obligaciones específicas.

Clasificación y Alcance del Estudio

El análisis se organiza en dos dimensiones:

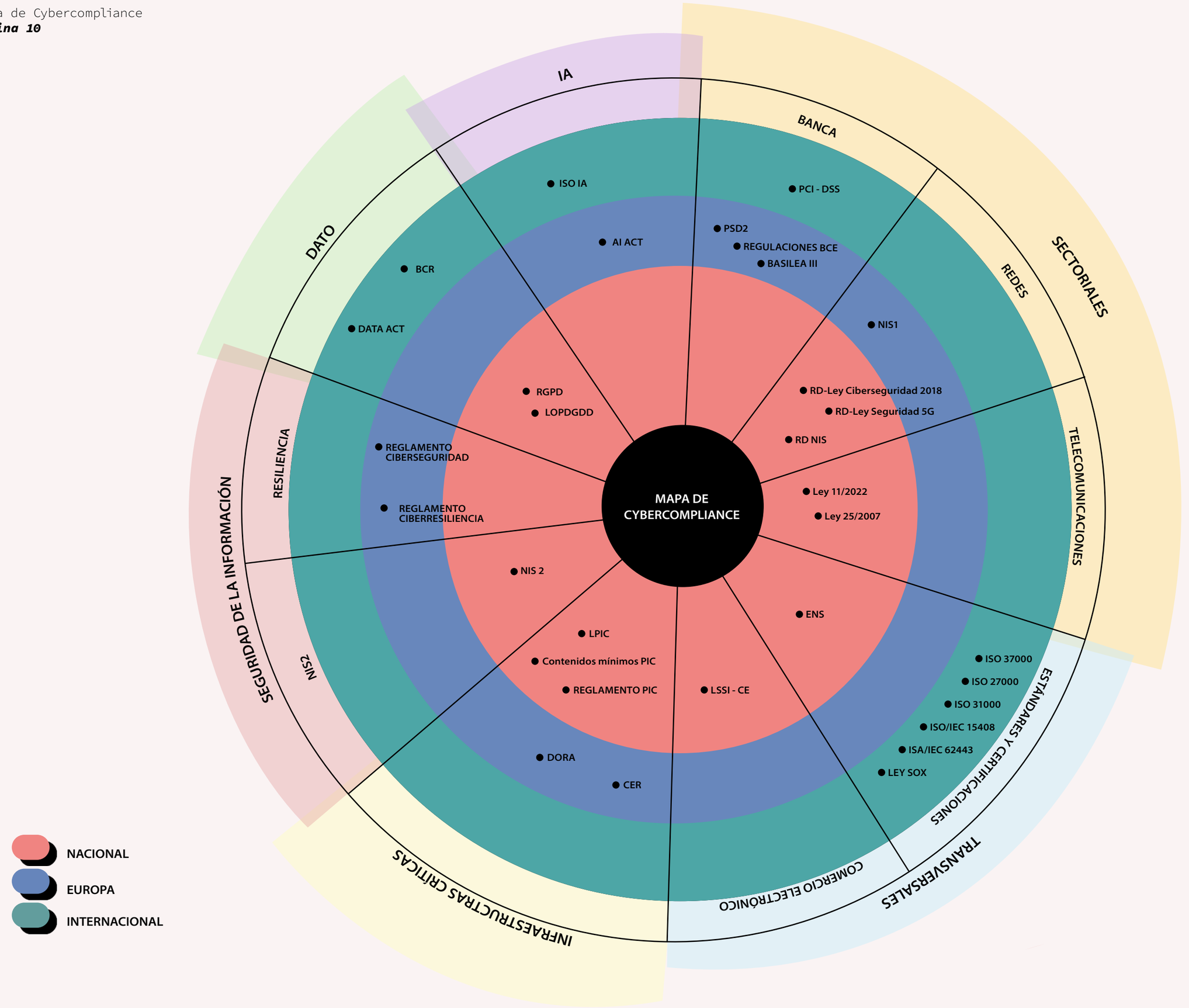
- **Temática**, agrupando normativas en áreas clave como inteligencia artificial, contratación pública, sector financiero, resiliencia entre otras.
- **Ámbito normativo**, diferenciando entre marcos nacionales, europeos e internacionales.

Además, hemos incorporado estándares reconocidos internacionalmente, como la familia **ISO/IEC 27000**, **NIST** y marcos nacionales como el **Esquema Nacional de Seguridad (ENS)**, que complementan las obligaciones legales con directrices técnicas y organizativas.

Un Entorno Normativo en Expansión

El número de normativas que imponen obligaciones en materia de seguridad de la información no deja de crecer, impulsado por la aceleración tecnológica y la necesidad de reforzar la confianza digital. La tendencia apunta a una **mayor densidad regulatoria**, especialmente desde el ámbito europeo, con iniciativas como el ***Reglamento de Ciberresiliencia (CRA)***, la ***Directiva NIS2*** o el ***AI Act***, que redefinirán el panorama del cumplimiento en los próximos años.

Con este estudio, ISMS Forum ofrece una primera aproximación que sirva como punto de partida para que las organizaciones puedan anticiparse, priorizar y planificar sus estrategias de cumplimiento, integrando la seguridad de la información como un elemento transversal y estratégico.


MAPA DE CYBERCOMPLIANCE
IA
ISO IA
AI ACT
BANCA
PCI - DSS
PSD2
REGULACIONES BCE
BASILEA III
SECTORIALES
REDES
NIS1
TELECOMUNICACIONES
RD-Ley Ciberseguridad 2018
RD-Ley Seguridad 5G
RD NIS
Ley 11/2022
Ley 25/2007
DATO
BCR
DATA ACT
RGPD
LOPDGDD
RESILIENCIA
REGLAMENTO CIBERSEGURIDAD
REGLAMENTO CIBERRESILIENCIA
SEGURIDAD DE LA INFORMACIÓN
NIS2
NIS 2
LPIC
Contenidos mínimos PIC
REGLAMENTO PIC
INFRAESTRUCTRAS CRÍTICAS
DORA
CER
COMERCIO ELECTRÓNICO
LSSI - CE
TRANSVERSALES
ENS
ESTANDARES Y CERTIFICACIONES
ISO 37000
ISO 27000
ISO 31000
ISO/IEC 15408
ISA/IEC 62443
LEY SOX
NACIONAL
EUROPA
INTERNACIONAL

Dato

- **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO**
- **Normas Corporativas Vinculantes** (artículo 47 del Reglamento General de Protección de Datos)
- **Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LO-PDGDD). Trasposición Reglamento UE (RGPD)
- **Reglamento (UE) 2023/2854, sobre normas armonizadas para un acceso justo a los datos y a su utilización (en adelante, "Reglamento de Datos" o "Data Act")**

NORMA/ ESTÁNDAR	**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 (Reglamento general de protección de datos) Directamente aplicable al no necesitar trasposición.
ALCANCE	**Espacio Económico Europeo (Unión Europea, Islandia, Noruega y Liechtenstein).** **Aplica a todos los sectores y no requiere trasposición pese a que el propio reglamento deje espacio para la regulación por parte de los países de aplicación (ej. edad para otorgar el consentimiento para el tratamiento de datos por parte de menores de edad)**
ÓRGANO SUPERVISOR	**CEPD (Comité Europeo de Protección de Datos), EDPS (European Data Protection Supervisor/Autoridad Europea de Protección de Datos) y autoridades de control nacionales. En España, la AEPD (Agencia Española de Protección de Datos)**
ESTADO	**Vigente**
Ámbito Subjetivo/Objetivo	**El ámbito de aplicación del RGPD es amplio y se divide en:** **1. Ámbito territorial:** Se aplica a todas las organizaciones, tanto dentro como fuera de la Unión Europea (UE), que procesen datos personales de residentes en la UE. Esto incluye empresas ubicadas fuera de la UE si ofrecen bienes o servicios a personas en la UE o realizan seguimientode su comportamiento. **2. Ámbito material:** Se aplica a cualquier tratamiento de datos personales, lo que incluye la recopilación, almacenamiento, uso, transmisión, y destrucción de datos relacionados con una persona identificada o identificable. Se refiere tanto a datos electrónicos como a datos en formato físico. **3. Ámbito subjetivo:** Afecta a todos los responsables y encargados del tratamiento de datos personales, como empresas, entidades públicas, instituciones educativas o de investigación, comercios y plataformas online y organizaciones sin ánimo de lucro, que actúen dentro del territorio de la UE o que traten los datos de individuos dentro de la UE. Por tanto, el RGPD tiene un ámbito de aplicación extraterritorial y cubre cualquier proceso de datos que afecte a la privacidad de los ciudadanos de la UE, independientemente de la ubicación del responsable del tratamiento.
Normativa/ Framework de referencia	*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. *Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE) * Real Decreto-ley 14/2019, de 31 de octubre, de medidas urgentes para la adaptación del ordenamiento jurídico español a la normativa de la Unión Europea sobre protección de datos * Esquema Nacional de Seguridad (ENS) * Ley 11/2022, de 28 de junio, General de Telecomunicaciones *Normativa sectorial * Instrucciones y Guías de la Agencia Española de Protección de Datos las cuáles son de aplicación directa para la prevención de sanciones

NORMA/ ESTÁNDAR	**Normas Corporativas Vinculantes** (artículo 47 del Reglamento General de Protección de Datos)
ALCANCE	**Internacional**
ÓRGANO SUPERVISOR	**Autoridad de Control competente en materia de protección de datos del Estado miembro europeo donde está ubicada la sede principal europea del grupo empresarial**
ESTADO	**Vigente**
Ámbito Subjetivo/Objetivo	**El objetivo es permitir la transferencia internacional de datos personales dentro de un grupo de empresas bajo un marco legal aprobado por la autoridad de protección de datos, garantizando que los datos reciban un nivel adecuado de protección independientemente del país de destino.**
Principales obligaciones	***Ser jurídicamente vinculantes para todos los miembros del grupo empresarial o unión de empresas** ***Garantizar los derechos de los titulares de los datos** ***Incluir los requisitos mínimos específicos como los establecidos en el artículo 47 del RGPD** ***Designar a un responsable de protección de datos (DPO o equivalente)** ***Establecer procedimientos de gobernanza interna para garantizar la vigilancia, auditoría y cumplimiento continuo de las normas corporativas vinculantes** ***Cumplir con las obligaciones en materia de notificación y transparencia** ***Garantizar la seguridad y protección técnica y organizativa**
Normativa/ Framework de referencia	**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 ("Reglamento General de Protección de Datos" o "RGPD")**

NORMA/ ESTÁNDAR	**Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Trasposición Reglamento UE (RGPD)
ALCANCE	**Nacional**
ÓRGANO SUPERVISOR	**AEPD**
ESTADO	**Vigente**
Ámbito Subjetivo/Objetivo	**"La presente ley orgánica tiene por objeto:** **a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.** **El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.** **b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución."**
Principales obligaciones	***Mantener un registro de actividades de tratamiento** ***Determinar las medidas de seguridad aplicables a los tratamientos identificados. Privacidad desde el diseño y por defecto** ***Designar el Delegado de Protección de Datos cuando sea aplicable** ***Amplía los derechos de los interesados: derecho a una información más detallada, portabilidad de los datos, limitación del tratamiento y a no ser objeto de decisiones individuales automatizadas.** ***Consentimiento expreso: declaración u otra acción afirmativa clara.** ***Comunicación Brechas de seguridad.** ***Gestión de terceros: la relación con los encargados de tratamiento** ***Códigos de conducta** ***Garantía de los derechos digitales** ***Sanciones.** ***Inclusión de la obligación de bloqueo de los datos (art. 32 LOPDGDD)**
Normativa/ Framework de referencia	***Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.** ***Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.** ***Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE)** *** Real Decreto-ley 14/2019, de 31 de octubre, de medidas urgentes para la adaptación del ordenamiento jurídico español a la normativa de la Unión Europea sobre protección de datos** *** Esquema Nacional de Seguridad (ENS)** *** Ley 11/2022, de 28 de junio, General de Telecomunicaciones** ***Normativa sectorial** *** Instrucciones y Guías de la Agencia Española de Protección de Datos las cuáles son de aplicación directa para la prevención de sanciones**

NORMA/ ESTÁNDAR	**Reglamento (UE) 2023/2854, sobre normas armonizadas para un acceso justo a los datos y a su utilización (en adelante, "Reglamento de Datos" o "Data Act")**
ALCANCE	Establece reglas sobre el intercambio de datos generados mediante el uso de productos conectados o servicios relacionados (por ejemplo, Internet de las cosas, maquinaria industrial) y permite a los usuarios acceder a los datos que generan. Afecta a fabricantes de productos conectados introducidos en la Unión y a proveedores de servicios relacionados, independientemente del lugar de dichos fabricantes, asimismo a titulares de datos, con independencia de su lugar de establecimiento, que pongan datos a disposición de los destinatarios de la Unión. Por tanto, el Data Act tiene un alcance extraterritorial al aplicarse a sujetos fuera de la UE si sus productos o servicios afectan a usuarios dentro de la Unión.
ÓRGANO SUPERVISOR	Los Estados Miembros designarán a una autoridad competente para garantizar la implementación del Reglamento. España aún no ha designado oficialmente a la autoridad competente. Cuando las obligaciones del Data Act afecten a la protección de datos, serán las autoridades nacionales competentes en materia de protección de datos.
ESTADO	La entrada formal en vigor del reglamento se produce el 11 de enero de 2024. El 12 de septiembre de 2025 se inició la aplicación general de la mayoría de las disposiciones. No obstante, la obligación de hacer accesibles para el usuario los datos de los productos y los datos de servicios relacionados será aplicable únicamente a los productos conectados y a los servicios relacionados con ellos introducidos en el mercado después del 12 de septiembre de 2026. Las empresas deberán asegurarse de que las cláusulas sobre acceso y uso de datos en sus contratos no sean abusivas. Esta obligación se aplicará: Desde el 12 de septiembre de 2025 para los contratos firmados a partir de esa fecha. Desde el 12 de septiembre de 2027 para los contratos firmados antes o el mismo 12 de septiembre de 2025, siempre que: a) tengan una duración indefinida, o b) terminen diez años o más después del 11 de enero de 2024.
Ámbito Subjetivo/Objetivo	El objetivo de la Data Act es impulsar la economía digital y eliminar obstáculos a la circulación de datos en el mercado común europeo. Para ello se centra en (i) los productos conectados y (ii) en los servicios relacionados, reconociendo una serie de obligaciones y límites aplicables al intercambio de datos que se generan por dichos productos y servicios relacionados. **Ámbito subjetivo:** Se aplica tanto a (i) datos obtenidos, generados o recogidos por un producto conectado y que se refieren a su rendimiento, uso o entorno (ii) datos del servicio relacionado, que representan la acción, inacción o eventos relacionados con el producto conectado durante la prestación de un servicio relacionado (iii) datos en bruto y preprocesados, acompañados de los metadatos necesarios para hacerlos comprensibles y utilizables. Se excluyen del ámbito de aplicación: (i) datos altamente enriquecidos, es decir, aquellos que no provienen directamente del funcionamiento de un producto o servicio conectado, sino que son el resultado de un proceso de tratamiento avanzado que transforma los datos en bruto en información con valor añadido nuevo (ii) Contenidos protegidos por derechos de propiedad intelectual o por secretos comerciales, con limitaciones. **El Data Act aplica a:** (i) Fabricantes de productos conectados y proveedores de servicios relacionados que se introduzcan en el mercado de la Unión Europea. (ii) Usuarios de los productos conectados o servicios relacionados. Esto es, a las personas físicas o jurídicas que utilicen el producto conectado, sean o no propietarios del mismo, o que reciban los servicios relacionados. (iii) Titulares de datos, entendiendo por ello a las personas físicas o jurídicas que tienen el derecho o la obligación de utilizar y poner los datos del producto conectado o servicio relacionado a disposición de los destinatarios de los datos. De forma general, los titulares de los datos son a su vez los fabricantes de los productos conectados y/o los proveedores de los servicios relacionados, aunque no necesariamente. También puede asumir dicho rol el proveedor de alguno de los componentes concretos del producto fabricado, existiendo, por tanto más de un titular de datos a la vez respecto a un producto. (iv) Destinatarios de los datos, a quienes el titular de datos comunique los datos del producto conectado o servicio relacionado a petición del usuario.

Principales obligaciones	**1.- Acceso a los datos generales:** Las empresas ("titulares de los datos") tienen la obligación legal, de poner los datos a disposición de otra empresa ("destinatario de los datos"), también en el contexto de los datos de IoT **2.- Intercambio de los datos:** Las condiciones del intercambio de información deben ser justas, razonables y no discriminatorias 3.-Diseño de los productos conectados: desde el 2026, los nuevos productos IoT deben incluir funcionalidades que permitan el acceso sencillo a los datos por parte de los usuarios. **4.- Atención a las cláusulas abusivas:** el Data Act establece una lista no exhaustiva de cláusulas que siempres se consideran abusivas (por ejemplo: aquellas que excluyen o limiten la responsabilidad de la parte que impuso unilateralmente la cláusula por actos intencionales o negligencia grave) y de cláusulas que se presumen abusivas (por ejemplo: las que limitan indebidamente las vías de recurso en caso de incumplimiento de las obligaciones contractuales) **5.-Acceso a los datos en caso de necesidad excepcional:** los organismos públicos podrán acceder a datos en poder de entidades privadas cuando exista una necesidad excepcional, es decir tanto emergencias públicas (catástrofes naturales o provocadas por el hombre, pandemias e incidentes de ciberseguridad) como situaciones no urgentes (por ejemplo: datos agregados y anonimizados de los sistemas GPS de los conductores para ayudar a optimizar los flujos de tráfico) **6.-Portabilidad en la nube:** los clientes de servicios de tratamiento de datos podrán cambiar de un proveedor a otro sin problemas **7.- Adopción de medidas para evitar accesos no autorizados:** los fabricantes y proveedores de IoT podrán introducir medidas tecnológicas de protección frente a usos no autorizados
Normativa/ Framework de referencia	El Data Act se integra en la Estrategia Digital de la UE de 2020 en materia de datos y completa al Reglamento de Gobernanza de Datos, el Reglamento de Mercados Digitales (DMA), la Ley de Servicios Digitales (DSA) y el Reglamento de Inteligencia Artificial (RIA).

Seguridad de la información

1. Resiliencia
2. NIS2

1. Resiliencia

- **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 y por el que se modifica el Reglamento (UE) n.o 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia).**

- **Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad»)**

NORMA/ ESTÁNDAR	**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 y por el que se modifica el Reglamento (UE) n.o 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia).**
ALCANCE	Europa y aplica a todos los fabricantes, importadores, distribuidores y representantes autorizados de productos hardware y software con elementos digitales.
ÓRGANO SUPERVISOR	Cada Estado miembro designará una o varias autoridades de vigilancia del mercado con el fin de garantizar la aplicación efectiva del presente Reglamento, que se deberán coordinar con la Agencia de la Unión Europea para la Ciberseguridad ("ENISA") y los Equipos de Respuesta a Incidentes de Seguridad Informática ("CSIRT") designados
ESTADO	Publicado el 20 de noviembre de 2024 y en vigor desde el 10 de diciembre de 2024. El RCR será plenamente aplicable el 11 de diciembre de 2027, aunque algunas disposiciones, como las obligaciones de información (artículo 14) y la notificación de organismos de evaluación (capítulo IV), serán obligatorias a partir de 2026.
Ámbito Subjetivo/Objetivo	Establecer requisitos de ciberseguridad para productos hardware y software con elementos digitales introducidos en la Unión Europea, abarcando dispositivos como sistemas operativos, asistentes virtuales, tarjetas inteligentes y dispositivos hardware. Exige que los productos se diseñen con altos estándares de seguridad, incluyendo la reducción de vulnerabilidades y la provisión de actualizaciones durante todo su ciclo de vida, además de fomentar la transparencia para decisiones informadas de los usuarios.
Principales obligaciones	**Aspectos clave:** - Los fabricantes deben incorporar medidas de seguridad desde el diseño, realizar evaluaciones de riesgos, mantener documentación técnica durante al menos diez años, garantizar el marcado CE y gestionar las vulnerabilidades con actualizaciones continuas. - Los importadores y distribuidores tienen la responsabilidad de verificar que los productos cumplan con los estándares de ciberseguridad y mantener su conformidad durante su comercialización. - Se introducen normas estrictas para productos críticos, que requieren evaluaciones rigurosas y mayor protección. - Se regula la seguridad de componentes de terceros, incluido el software de código abierto, y se establece que, en ciertos casos, los importadores y distribuidores asumirán las obligaciones de los fabricantes si comercializan productos bajo su marca o los modifican sustancialmente. **Notificaciones:** Los fabricantes deben notificar a la Agencia de la Unión Europea para la Ciberseguridad ("ENISA") y al Equipo de Respuesta a Incidentes de Seguridad Informática ("CSIRT") designado, vulnerabilidades explotadas activamente e incidentes graves, definidos como aquellos que comprometen funciones sensibles, datos o introducen código malicioso. Las notificaciones se realizan en tres etapas: una advertencia temprana dentro de las 24 horas, un informe intermedio en 72 horas con medidas correctivas, y un informe final en un mes con detalles exhaustivos. En casos excepcionales, se permite un aplazamiento por motivos de ciberseguridad. Los usuarios afectados deben ser informados directamente por los fabricantes o, en su defecto, por los CSIRTs. **Confidencialidad y sanciones:** Se establecen condiciones estrictas para garantizar el cumplimiento de las disposiciones sin comprometer información sensible, derechos de propiedad intelectual ni la seguridad nacional. Las sanciones incluyen multas de hasta 15 millones de euros o el 2,5% del volumen de negocios anual mundial por infracciones graves a los requisitos de ciberseguridad, y sanciones menores para el incumplimiento de otras obligaciones o la provisión de información engañosa La cuantía de las multas considera factores como la gravedad y duración de la infracción, con exenciones para pequeñas empresas y administradores de software de código abierto en ciertos casos. **Implementación:** Las empresas dispondrán de un período de transición para adaptar sus productos existentes, minimizando interrupciones. Los operadores económicos, en particular los fabricantes, deben llevar a cabo un análisis de brechas para identificar deficiencias en sus medidas actuales, con un enfoque basado en riesgos, incluyendo los de la cadena de suministro, y fortaleciendo su capacidad para gestionar vulnerabilidades.
Normativa/ Framework de referencia	Comunicación conjunta de la Comisión y del alto representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 16 de diciembre de 2020, titulada «Estrategia de Ciberseguridad de la UE para la Década Digital», las Conclusiones del Consejo, de 2 de diciembre de 2020, sobre la ciberseguridad de los dispositivos conectados, y de 23 de mayo de 2022, sobre el desarrollo de la posición de la Unión Europea en materia de ciberseguridad y la Resolución del Parlamento Europeo, de 10 de junio de 2021, sobre la Estrategia de Ciberseguridad de la UE para la Década Digital. Reglamento (UE) n.o 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia)

NORMA/ ESTÁNDAR	**Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad»)**
ALCANCE	Europa
ÓRGANO SUPERVISOR	ENISA
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	El Reglamento fija el mandato y funciones de ENISA, incluyendo su papel en garantizar la transparencia y la gestión confidencial de la información en el ámbito de la ciberseguridad. Además, también establece las directrices para la creación y gestión del esquema europeo de certificación de la ciberseguridad, que es un marco armonizado para certificar productos, servicios y procesos TIC en Europa.
Principales obligaciones	Se establecen obligaciones para ENISA relativas a realizar sus actividades con transparencia, confidencialidad. Asimismo, se establecen las directrices para la creación del esquema europeo de certificación de la ciberseguridad.
Normativa/ Framework de referencia	Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC).

2. NIS2

- **Directiva (UE) 2022/2555 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, por la que se modifican el Reglamento (UE) n. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS2/SRI 2)**

NORMA/ ESTÁNDAR	**Directiva (UE) 2022/2555 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, por la que se modifican el Reglamento (UE) n. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS2/SRI 2)**
ALCANCE	Aplica a los estados miembros de la UE, y a las entidades públicas y privadas consideradas esenciales o importantes que operen dentro de la UE, o que presten servicios esenciales o importantes dentro de la UE. Se excepcionan aquellos organismos que operen en el ámbito de la defensa y seguridad nacional. Los tipos de entidades afectadas serán: **Entidades esenciales:** Energía, Transporte, Banca, Mercados financieros, Sector sanitario, Agua potable y tratamiento de aguas residuales, Infraestructuras digitales, Gestión de Servicios TIC, Administración pública (a excepción del poder judicial, parlamentos y bancos centrales), Espacio. **Entidades importantes:** Servicios postales y de mensajería; Gestión de residuos; Fabricación, producción y distribución de sustancias químicas; Producción, transformación y distribución de alimentos; Fabricación, Proveedores de Servicios Digitales; e Investigación Aplicará a los sectores mencionados siempre que se trate de medianas y grandes empresas de acuerdo a la Recomendación 2003/361/CE. Y con independencia a su tamaño cuando: - Los servicios son prestados por: i) proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público; ii) prestadores de servicios de confianza; iii) registros de nombres de dominio de primer nivel y proveedores de servicios de sistema de nombres de dominio; - La entidad sea el único proveedor en un Estado miembro de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas; - Una perturbación del servicio prestado por la entidad pudiera tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública; o pudiera inducir riesgos sistémicos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo; - La entidad sea crítica a la luz de su importancia específica a nivel nacional o regional para el sector o tipo de servicio en concreto o para otros sectores interdependientes en el Estado miembro; - La entidad sea una entidad de la Administración pública (en los supuestos definidos en el artículo 2.2 (f)) - Sean entidades que se identifiquen como entidades críticas con arreglo a la Directiva (UE) 2022/2557
ÓRGANO SUPERVISOR	Cada Estado miembro de la UE debe designar (en su transposición) al menos una autoridad nacional competente que se encargue de la supervisión general de la implementación de la directiva. A nivel europeo, se establecen diferentes organismos de cooperación: - Grupo de cooperación (NIS Coperation Group) - Red de CSIRT - Red EU-CyCLONe
ESTADO	Se trata de una Directiva, por tanto los Estados Miembros deberán transponer esta norma a su legislación interna. El período de transposición finalizó el 17/10/2024. Por tanto es aplicable desde el 18/10/2024. La mayor parte de Estados Miembros aún no han transpuesto la normativa, entre ellos, España
Ámbito Subjetivo/Objetivo	El principal objetivo de la Directiva NIS2 es fortalecer la ciberseguridad en toda la Unión Europea, mejorando la resiliencia de los sistemas y redes de información de las entidades que prestan servicios esenciales o importantes para la economía y la sociedad. Esta directiva busca garantizar una mayor protección contra las ciberamenazas y mejorar la capacidad de respuesta ante incidentes de seguridad en todos los sectores clave. En este sentido, podemos enumerar como objetivos clave: - Mejorar la ciberseguridad de sectores clave. - Establecer requisitos más estrictos de ciberseguridad. - Establecer mecanismos de notificación de incidentes. - Aumentar la cooperación y coordinación entre los Estados Miembros. - Homogeneizar los estándares de seguridad. - Mejorar la resiliencia de las cadenas de suministro. - Fomentar la cultura de la ciberseguridad.

Principales obligaciones	**1. Gobernanza y Responsabilidades de la Dirección:** Los órganos de dirección de las entidades esenciales e importantes deben: *Aprobar las medidas de gestión de riesgos de ciberseguridad. *Supervisar su implementación. *Ser responsables de la eficacia de estas medidas. Además, deben asegurarse de que los miembros de la dirección reciban formación periódica en ciberseguridad y proporcionar formación similar a los empleados **2. Medidas para la Gestión de Riesgos de Ciberseguridad:** Las empresas deben adoptar medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos de ciberseguridad (enfoque basado en riesgos). Incluye desde la definición de políticas de seguridad y la gestión de incidentes, hasta la seguridad de la cadena de suministro. (ENISA, y el propio CCN, están desarollando perfiles de cumplimiento basados en estándares, Ver Perfil de Cumplimiento Especifico CCN-STIC 892) **3. Notificación de Incidentes de Ciberseguridad:** Las empresas deben notificar a las autoridades competentes y a los destinatarios de sus servicios sobre incidentes de ciberseguridad que tengan un impacto significativo en la prestación de sus servicios. La notificación inicial deberá realizarse a las 24 horas desde que se tuvo conocimiento del incidente. La notificación intermedia a las 72 horas y el informe final deberá ser enviado en el plazo de 1 mes.
Normativa/ Framework de referencia	NIS2 es la evolución y actualización de la directiva Directiva NIS1 (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

Inteligencia Artificial

- **ISO 42001:2023 - Gestión de Sistemas de IA**

- **Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).**

NORMA/ ESTÁNDAR	**ISO 42001:2023 - Gestión de Sistemas de IA**
ALCANCE	Internacional
ÓRGANO SUPERVISOR	No se establece ningún órgano específico
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	Se aplica a cualquier tipo de organización que busque desarrollar, proveer o utilizar sistemas de IA o productos y servicios basados en IA, enfocándose en garantizar un uso responsable, ético, transparente y seguro de los sistemas de inteligencia artificial.
Principales obligaciones	Las obligaciones estipuladas en la norma, que establece un Sistema de Gestión de la Inteligencia Artificial (SGIA), incluyen lo siguiente: *Establecer, implementar, mantener y mejorar continuamente un sistema de gestión de IA en la organización que asegure el uso responsable y ético de la inteligencia artificial. *Definir roles y responsabilidades claras para la gestión de la IA, incluyendo el compromiso de la alta dirección para asignar recursos y definir políticas de gestión. *Evaluar y gestionar riesgos asociados a los sistemas de IA, como sesgos algorítmicos, fallos de seguridad y otros impactos negativos potenciales. *Desarrollar procesos específicos para el diseño, despliegue, supervisión y mantenimiento de los sistemas de IA, garantizando su fiabilidad, transparencia y responsabilidad. *Documentar procesos y asegurar la trazabilidad y rendición de cuentas para fomentar la transparencia en el uso de IA. *Capacitar y concienciar al personal sobre la importancia de una gestión responsable de la IA, con programas continuos de formación sobre riesgos, requisitos normativos y buenas prácticas. *Implementar mecanismos de supervisión y evaluación continuos, incluyendo auditorías internas y revisiones periódicas para asegurar la eficacia del sistema de gestión de IA. *Cumplir con las normativas legales y éticas aplicables, complementando requisitos regulatorios como el Reglamento de Inteligencia Artificial de la Unión Europea.
Normativa/ Framework de referencia	Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial

NORMA/ ESTÁNDAR	**Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).**
ALCANCE	Aplica agentes públicos y privados, dentro y fuera de la UE, en la medida en que afecte a la introducción de la IA en el mercado de la UE o afecte a personales establecidas en la UE. Con las excepciones establecidas para los Estados en materia de seguridad.
ÓRGANO SUPERVISOR	El Supervisor Europeo de Protección de Datos.
ESTADO	En vigor (desde 1 de agosto de 2024) Será aplicable a partir del 2 de agosto de 2026. a) los capítulos I y II serán aplicables a partir del 2 de febrero de 2025; b) el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII y el artículo 78 serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101; c) el artículo 6, apartado 1, y las obligaciones correspondientes del presente Reglamento serán aplicables a partir del 2 de agosto de 2027.
Ámbito Subjetivo/Objetivo	**Art. 2.** a) los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA o que introduzcan en el mercado modelos de IA de uso general en la Unión, con independencia de si dichos proveedores están establecidos o ubicados en la Unión o en un tercer país; b) los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión; c) los proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión; d) los importadores y distribuidores de sistemas de IA; e) los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca; f) los representantes autorizados de los proveedores que no estén establecidos en la Unión; g) las personas afectadas que estén ubicadas en la Unión.
Principales obligaciones	*Sistema de gestión de riesgos *Transparencia y comunicación de información a los usuarios *Vigilancia humana *Registros, documentación técnica *Precisión, solidez y ciberseguridad
Normativa/ Framework de referencia	Recomendación sobre la ética de la inteligencia artificial (2021) Principios de la OCDE sobre Inteligencia Artificial (2019) Principios de la Declaración de la Cumbre del G20 sobre IA (2019) Guía para la construcción de una IA ética (2020) del Foro Económico Mundial.

Infraestructuras críticas

- **Directiva (UE) 2022/2557 o la Directiva de Resiliencia de las Entidades Críticas (CER, por sus siglas en inglés: Critical Entities Resilience Directive)**
- **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)**
- **Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. (Ley de Protección de Infraestructuras Críticas, LPIC)**
- **Real Decreto 704/2011 aprueba el Reglamento de Protección de las Infraestructuras Críticas, desarrollado por la Ley 8/2011**

NORMA/ ESTÁNDAR	**Directiva (UE) 2022/2557 o la Directiva de Resiliencia de las Entidades Críticas (CER, por sus siglas en inglés: Critical Entities Resilience Directive)** **La Directiva busca garantizar un enfoque coordinado y eficiente en toda la Unión Europea para proteger las infraestructuras críticas frente a riesgos crecientes, tales como desastres naturales, ciberataques, pandemias y actos malintencionados.** **En este contexto, se exige a los Estados miembros que identifiquen las entidades críticas nacionales y que desarrollen estrategias y planes de acción para su protección y resiliencia.**
ALCANCE	El alcance de la Directiva (UE) 2022/2557 abarca la identificación, protección y mejora de la resiliencia de las entidades críticas en los Estados miembros de la Unión Europea que prestan servicios esenciales para la sociedad y la economía. Esta Directiva introduce un enfoque integral para gestionar los riesgos y fortalecer la capacidad de estas entidades frente a interrupciones significativas, ya sean de origen natural, accidental, intencionado o derivadas de ciberamenazas. **Alcance de la Directiva en el ámbito geográfico:** aplica a todos los Estados miembros de la Unión Europea, exigiéndoles desarrollar estrategias nacionales de resiliencia y cooperar entre sí, especialmente en el caso de amenazas transfronterizas. **Alcance de la directiva en el ámbito sectorial:** se aplica a 11 sectores esenciales y subsectores que tienen un papel crucial para la sociedad y la economía. Estos sectores son: Energía, transporte, Banca, Infraestructura de los mercados financieros, Salud, Agua potable, Gestión de aguas residuales, Infraestructura digital, Administración pública, Producción, Procesamiento y distribución de alimentos, Espacio **Alcance de la directiva: entidades críticas, quiénes son:** se refiere a las entidades que operan dentro de los sectores esenciales y cuya interrupción tendría un impacto significativo en la sociedad, la economía o la seguridad nacional. Estas entidades deben ser identificadas y designadas por los Estados miembros como ""entidades críticas"". **Alcance de la directiva: riesgos y amenazas cubiertos:** Incluye riesgos naturales (terremotos, inundaciones, pandemias, etc.), riesgos accidentales (fallos técnicos, cortes eléctricos), riesgos derivados de actos intencionados (ataques terroristas, sabotajes) y ciberamenazas. **Alcance de la directiva: Cooperación y coordinación:** Impulsa la colaboración entre los Estados miembros para gestionar amenazas transfronterizas y desarrollar un enfoque común para proteger las entidades críticas en toda la UE. **Alcance de la directiva: Exclusiones:** No se aplica a las entidades que operan exclusivamente en sectores militares o de defensa, ya que estas áreas tienen su propia regulación específica dentro del marco europeo."
ÓRGANO SUPERVISOR	La Directiva (UE) 2022/2557 establece que los órganos supervisores son, en primera instancia, las autoridades competentes de los Estados miembros. Cada Estado miembro debe designar una o varias autoridades nacionales encargadas de supervisar la implementación de la Directiva y coordinar las medidas necesarias para garantizar la resiliencia de las entidades críticas. **1. Características del órgano supervisor:** - Autoridades nacionales competentes: cada Estado miembro debe nombrar una autoridad (o varias) para supervisar la correcta aplicación de la Directiva en su territorio.Estas autoridades son responsables de: *Identificar y designar las entidades críticas dentro de su jurisdicción.* *Supervisar el cumplimiento de las obligaciones impuestas a las entidades críticas, como la elaboración de planes de resiliencia.* *Realizar evaluaciones regulares de riesgos y amenazas.* *Coordinar con otras autoridades competentes en la UE, especialmente en el caso de amenazas transfronterizas.* - **Punto de contacto único: cada Estado miembro debe designar un punto de contacto único (Single Point of Contact, SPOC) que actúe como enlace entre las autoridades nacionales y la Comisión Europea, así como con otros Estados miembros. Este punto de contacto facilita la cooperación transfronteriza y el intercambio de información sobre riesgos, amenazas y mejores prácticas.** **2. Papel de la Comisión Europea:** aunque los Estados miembros tienen la responsabilidad principal, la Comisión Europea desempeña un papel de supervisión y apoyo. Esto incluye: *Supervisar la implementación general de la Directiva a nivel de la UE.* *Promover la cooperación entre Estados miembros.* *Coordinar la respuesta en caso de amenazas o riesgos que afecten a múltiples países.* *Solicitar informes regulares a los Estados miembros sobre el progreso en la aplicación de la Directiva.* **3. Cooperación internacional:** además de las autoridades nacionales y la Comisión, se fomenta la cooperación con organismos de la UE especializados, como la Agencia de la Unión Europea para la Ciberseguridad (ENISA), que apoya la implementación de medidas relacionadas con la ciberseguridad en las entidades críticas. En resumen, el órgano supervisor directo es la autoridad nacional competente designada por cada Estado miembro, que actúa bajo la coordinación de la Comisión Europea para garantizar la coherencia y eficacia en toda la Unión.
ESTADO	La Directiva (UE) 2022/2557, relativa a la **resiliencia de las entidades críticas**, tiene el siguiente estado actual: ***Vigente*** La Directiva entró en vigor el 16 de enero de 2023, 20 días después de su publicación en el Diario Oficial de la Unión Europea (DOUE) el 27 de diciembre de 2022. ***En transposición:*** Los Estados miembros de la Unión Europea tienen hasta el 17 de octubre de 2024 para transponer la Directiva a sus respectivas legislaciones nacionales. Durante este período, los Estados deben desarrollar o adaptar sus marcos normativos para cumplir con las disposiciones establecidas. ***En preparación:*** Los Estados miembros están actualmente trabajando en la identificación de las entidades críticas y la actualización de sus estrategias nacionales de resiliencia. ***Plazo de implementación:*** fecha límite de transposición: 17 de octubre de 2024. A partir de esa fecha, las disposiciones de la Directiva deben estar plenamente integradas en las legislaciones nacionales y aplicarse en los Estados miembros. Aplicación escalada: Aunque el plazo de implementación es general, las disposiciones específicas pueden aplicarse de forma escalonada, dependiendo de la capacidad de cada Estado miembro para cumplir con las obligaciones. Por ejemplo, algunos sectores o entidades críticas pueden ser priorizados en función de su importancia estratégica o vulnerabilidad frente a riesgos. ***Próximos pasos:*** Los Estados miembros deben: **Designar autoridades nacionales competentes y puntos de contacto únicos.* **Realizar evaluaciones de riesgos y amenazas nacionales.* **Establecer estrategias nacionales de resiliencia.* **Identificar y notificar a las entidades críticas afectadas.* En el caso de la adopción de una estrategia para la resiliencia de las entidades críticas y de la identificación de las entidas críticas para los sectores y subsectores de la Directiva, los Estados Miembros tienen hasta el 17 de julio de 2026. La Comisión Europea supervisará y apoyará la transposición y garantizará que los Estados miembros cumplan con los plazos establecidos.

Ámbito Subjetivo/ Objetivo	**Objetivo de la norma:** La Directiva busca garantizar la resiliencia de las entidades críticas en la Unión Europea, protegiendo su capacidad para prevenir, resistir, responder y recuperarse de incidentes disruptivos. Esto se centra en mantener la continuidad de los servicios esenciales para la sociedad y la economía frente a amenazas naturales, accidentales, intencionadas o cibernéticas. La norma promueve un enfoque coordinado entre los Estados miembros y establece requisitos claros para mejorar la planificación, supervisión y cooperación en la protección de infraestructuras críticas. Ámbito subjetivo (a quién se aplica): **Entidades críticas:** Empresas y organizaciones que operan en sectores esenciales, cuya interrupción afectaría significativamente a la seguridad, la salud o la economía. **Estados miembros:** Responsables de identificar entidades críticas, supervisar su cumplimiento y establecer estrategias nacionales de resiliencia. Ámbito objetivo (qué se aplica): **Sectores cubiertos:** Energía, transporte, salud, agua potable, gestión de aguas residuales, banca, infraestructura de mercados financieros, infraestructura digital, alimentos, administración pública y espacio. **Obligaciones:** Evaluación de riesgos, diseño de planes de resiliencia, cooperación transfronteriza y supervisión del cumplimiento por parte de las autoridades nacionales. En resumen, se aplica a todos los sectores esenciales definidos y a los Estados miembros que deben garantizar la aplicación de la norma en sus territorios.
Principales obligaciones	<u>Principales obligaciones para los sujetos obligados:</u> **Para los Estados Miembros:** Identificación de entidades críticas: Determinar las entidades cuya interrupción tendría un impacto significativo en la seguridad nacional, la salud pública o la economía. Evaluaciones de riesgos: Realizar análisis periódicos de amenazas y vulnerabilidades relacionadas con los sectores críticos. Estrategia nacional de resiliencia: Diseñar y mantener una estrategia que establezca medidas para prevenir y mitigar riesgos. Supervisión y designación de autoridades: Designar autoridades competentes para supervisar el cumplimiento de la Directiva. Establecer puntos de contacto únicos para la coordinación a nivel europeo. Cooperación internacional: Colaborar con otros Estados miembros y la Comisión Europea en el manejo de amenazas transfronterizas. **Para las entidades críticas:** Planes de resiliencia: Elaborar, implementar y mantener planes específicos para garantizar la continuidad del servicio en caso de incidentes. Gestión de riesgos: Evaluar riesgos relacionados con su infraestructura y aplicar medidas preventivas adecuadas. Notificación de incidentes: Informar a las autoridades nacionales sobre interrupciones significativas o amenazas que afecten sus operaciones. Colaboración con las autoridades: Designar responsables de enlace para interactuar con las autoridades competentes y facilitar la supervisión. <u>**Consecuencias para los sujetos obligados:**</u> **Para los Estados Miembros:** Incumplimiento de la transposición: Pueden enfrentarse a procedimientos de infracción por parte de la Comisión Europea. Impacto en la seguridad nacional: Falta de cumplimiento podría llevar a una mayor vulnerabilidad frente a amenazas y a la interrupción de servicios esenciales. **Para las entidades críticas:** Sanciones: Los Estados miembros deben establecer sanciones proporcionales y disuasorias para las entidades que no cumplan con las obligaciones, como multas económicas o medidas correctivas. Impacto operativo y reputacional: La falta de planes de resiliencia o la mala gestión de riesgos puede resultar en interrupciones graves que afecten su reputación y funcionamiento. Responsabilidad legal: En casos de negligencia que afecten la prestación de servicios esenciales, las entidades podrían enfrentar responsabilidades legales adicionales. En resumen, las obligaciones buscan garantizar la continuidad de los servicios esenciales, mientras que las consecuencias del incumplimiento varían desde sanciones económicas hasta repercusiones legales y operativas."
Normativa/ Framework de referencia	La Directiva (UE) 2022/2557 está inspirada y fundamentada en varios marcos normativos previos de la Unión Europea, así como en iniciativas globales relacionadas con la protección de infraestructuras críticas y la gestión de riesgos. A continuación, se destacan las normas y frameworks más relevantes: **Normativa de referencia previa:** <u>Directiva 2008/114/CE:</u> Tema: Identificación y designación de infraestructuras críticas europeas (ICE) en los sectores de energía y transporte. Relación: La Directiva 2022/2557 sustituye a la 2008/114/CE, ampliando su alcance a más sectores y enfocándose en la resiliencia en lugar de solo la protección física. <u>Directiva (UE) 2016/1148 (Directiva NIS):</u> Tema: Seguridad de las redes y sistemas de información en la UE. Relación: La Directiva NIS establece requisitos de ciberseguridad para operadores de servicios esenciales, que se complementan con los requisitos de resiliencia de la Directiva 2022/2557. <u>Reglamento (UE) 2019/881 (Reglamento de Ciberseguridad):</u> Tema: Fortalecimiento de la seguridad cibernética en la UE y el papel de la ENISA. Relación: Proporciona un marco específico para las amenazas cibernéticas, que se considera en el contexto más amplio de la resiliencia de las entidades críticas. **Normativa o frameworks que la desarrollan o complementan:** <u>Directiva NIS2 (Directiva (UE) 2022/2555):</u> Tema: Ampliación de la ciberseguridad a más sectores y mejora de la gestión de riesgos. Relación: Junto con la Directiva 2022/2557, forma un marco integral para la seguridad física y digital de infraestructuras críticas en la UE. **Reglamentos sectoriales específicos:** Ejemplo: Reglamento (UE) 2021/1229 sobre sistemas financieros y su infraestructura. Relación: Estas normativas sectoriales complementan los requisitos generales de resiliencia establecidos en la Directiva 2022/2557. Inspiraciones internacionales: Aunque no forman parte del marco normativo de la UE, algunas iniciativas globales han servido de referencia, como los Principios de Protección de Infraestructuras Críticas de la OCDE y el enfoque de resiliencia adoptado por el Departamento de Seguridad Nacional de los EE. UU. En síntesis, la Directiva (UE) 2022/2557 se basa en el marco previo de la Directiva 2008/114/CE, se complementa con la Directiva NIS2, y se desarrolla en sinergia con regulaciones específicas sectoriales y de ciberseguridad, estableciendo un sistema integral de resiliencia en toda la Unión Europea.

NORMA/ ESTÁNDAR	**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)**
ALCANCE	Europa
ÓRGANO SUPERVISOR	Autoridades Europeas de Supervisión (AES) compuestas por: *EBA (Autoridad Bancaria Europea) *ESMA (Autoridad Europea de Valores y Mercados) *EIOPA (Autoridad Europea de Seguros y Pensiones de Jubilación) Las AES se coordinarán con el BCE (Banco Central Europeo). Asimismo, los Estados Miembros designarán a las autoridades nacionales competentes (en el caso de España: CNMV, Banco de España y DGSFP)
ESTADO	Vigente desde 17 de enero de 2025
Ámbito Subjetivo/Objetivo	**Es de aplicación a diferentes entidades financieras (bancos, entidades de crédito, empresas de seguros y reaseguros, sociedades de inversión y gestoras, entidades de dinero electrónico etc) Regula la resiliencia operativa digital de las entidades del sector financiero** **Garantiza que puedan resistir, responder y recuperarse ante ciberincidentes, fallos tecnológicos y disrupciones** **Busca armonizar los requisitos TIC en toda la UE, eliminando divergencias entre sectores y países**
Principales obligaciones	***Gestión de riesgos TIC:** Implantar un marco de gestión de riesgos tecnológicos que inluya la identificación, protección, detección, respuesta y recuperación. ***Gestión de incidentes TIC:** Obligación de detectar, clasificar y gestionar incidentes TIC; Informar a las autoridades de forma armonizada (plazo máximo: 24 horas para incidentes graves); Informar también a los clientes cuando sea necesario. *Requiere pruebas periódicas de ciberresiliencia (penetración, escenarios adversos). Las entidades significativas deben realizar pruebas avanzadas como Threat-Led Penetration Testing (TLPT). ***Gestión de riesgos de terceros TIC:** Obligación de controlar y supervisar a proveedores TIC externos críticos (cloud, software, etc.). Se exige: - Evaluación de riesgos antes de contratar. - Cláusulas contractuales mínimas obligatorias. - Seguimiento continuo. - Notificación de subcontrataciones. - Intercambio de información sobre ciberamenazas ***Fomenta el intercambio voluntario de información sobre amenazas, incidentes y vulnerabilidades entre entidades financieras.**
Normativa/ Framework de referencia	*NTR (RTS) sobre el marco de gestión de riesgos de las TIC y sobre el marco simplificado de gestión de riesgos *NTR (RTS) sobre criterios para la clasificación de incidentes relacionados con las TIC *NTR (RTS) para especificar la notificación de incidentes graves relacionados con las TIC *NTR (RTS)/ITS para especificar pruebas de penetración basadas en amenazas *NTR (RTS) para especificar la política sobre los servicios TIC prestados por terceros ***EIOPA-BoS-20_600** - Directrices sobre gobernanza y seguridad de las tecnologías de la información y de las comunicaciones y EIOPA-BoS-20-002 - Directrices sobre la externalización a proveedores de servicios en la nube se subsumen en el marco general establecido por DORA

NORMA/ ESTÁNDAR	**Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. (Ley de Protección de Infraestructuras Críticas, LPIC)**
ALCANCE	Nacional, aquellas empresas públicas o privadas que hayan sido designadas infraestructuras críticas por los órganos correspondientes
ÓRGANO SUPERVISOR	CNPIC, OCC
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	**Esta Ley tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población.**
Principales obligaciones	El Título I se destina a las definiciones de los términos acuñados por la Directiva 2008/114/CE, así como a establecer las cuestiones relativas al ámbito de aplicación y objeto. El Título II se dedica a regular los órganos e instrumentos de planificación que se integran en el Sistema de Protección de las Infraestructuras Críticas. El Título III establece, finalmente, las medidas de protección y los procedimientos que deben derivar de la aplicación de dicha norma: * Nombramiento del Responsable de Seguridad y Enlace, así como de los Delegados de las Infraestructuras Críticas * Definición, desarrollo e implementación de los Planes de Seguridad del Operador, y los Planes de Protección Específicos de cada una de las infraestructuras críticas * Los sistemas, las comunicaciones y la información relativa a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.
Normativa/ Framework de referencia	* 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 * Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

NORMA/ ESTÁNDAR	**El Real Decreto 704/2011 aprueba el Reglamento de Protección de las Infraestructuras Críticas, desarrollado por la Ley 8/2011. Establece normas y procedimientos para la protección de infraestructuras vitales, definiendo responsabilidades y mecanismos para garantizar su seguridad**
ALCANCE	**Nacional. Establece el marco normativo para la protección de infraestructuras críticas, abarcando tanto el sector público como el privado. Identifica y clasifica las infraestructuras críticas que son esenciales para el funcionamiento de la sociedad. Incluye varios niveles de planes, como el Plan Nacional de Protección, Planes Estratégicos Sectoriales, Planes de Seguridad del Operador y Planes de Protección Específicos. Establece mecanismos de comunicación entre los operadores críticos y las administraciones públicas para garantizar una respuesta eficaz ante amenazas. El objetivo es el de garantizar la seguridad y resiliencia de las infraestructuras críticas frente a diversas amenazas, incluyendo el terrorismo y otros actos delictivos."**
ÓRGANO SUPERVISOR	**Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). El CNPIC es responsable de impulsar, coordinar y supervisar todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas en España. Este centro depende del Secretario de Estado de Seguridad del Ministerio del Interior**
ESTADO	**Vigente**
Ámbito Subjetivo/Objetivo	**Garantizar la seguridad y resiliencia de las infraestructuras críticas frente a diversas amenazas, incluyendo el terrorismo y otros actos delictivos.**
Principales obligaciones	**1. Elaboración de planes de protección 2. Planes estratégicos Sectoriales 3. Planes de seguridad de operador 4. Planes de protección específicos 5. Designación de Responsables de Seguridad 6. Comunicación y coordinación 7. Evaluación y actualización**
Normativa/ Framework de referencia	**El Real Decreto 704/2011 se apoya principalmente en la Ley 8/2011, de 28 de abril. El decreto cumple con la Directiva 2008/114/CE del Consejo de la Unión Europea.**

Sectoriales

1. Bancaria
2. Telecomunicaciones
3. Redes

1. Bancaria

- **PCI DSS - Norma de Seguridad para empresas que manejan tarjetas de credito y debito. Diseñada para proteger la información de los titulares de tarjetas y reducir el fraude.**
- **Directiva (UE) 2015/2366, también conocida como PSD2 (Payment Services Directive 2**
- **Regulaciones del Banco Central Europeo**
- **Basilea III - Marco Regulador Internacional para Bancos como respuesta a la crisis financiera de 2007-2009**

NORMA/ ESTÁNDAR	**PCI DSS - Norma de Seguridad para empresas que manejan tarjetas de credito y debito. Diseñada para proteger la información de los titulares de tarjetas y reducir el fraude.**
ALCANCE	Aplica a nivel mundial a toda empresa que almacene, procese o transmita datos de tarjeta de pago, o a toda empresa proveedora de servicios que pueda afectar de forma directa o indirecta la seguridad de los mismos.
ÓRGANO SUPERVISOR	PCI Council Visa, American Express, MasterCard, JCB, Discover, Union Pay
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	El objetivo de PCI DSS es garantizar la protección de los datos de titulares de tarjetas de crédito y débito, reducir el riesgo de fraude y proteger las transacciones de pago en cualquier entorno que maneje estos datos. La norma busca establecer un conjunto unificado de requisitos de seguridad para que las organizaciones protejan adecuadamente la información confidencial de los titulares de las tarjetas durante su almacenamiento, procesamiento y transmisión. Ámbito subjetivo y objetivo PCI DSS se aplica a todas las entidades que aceptan, procesan, almacenan o transmiten datos de titulares de tarjetas, incluyendo comercios, bancos adquirentes, procesadores de pagos y proveedores de servicios. Además, cubre cualquier sistema o componente que interactúe directa o indirectamente con estos datos, incluyendo redes, servidores, aplicaciones y dispositivos físicos.
Principales obligaciones	*Cumplimiento con los requisitos de seguridad *Auditorías y evaluaciones periódicas *Multas por incumplimiento *Responsabilidad ante brechas de seguridad *Implementación de medidas correctivas *Suspensión o revocación de la capacidad de procesar pagos
Normativa/ Framework de referencia	ISO 27001, COBIT, CIS, NIST

NORMA/ ESTÁNDAR	**La Directiva (UE) 2015/2366, también conocida como PSD2 (Payment Services Directive 2), es una normativa de la Unión Europea que regula los servicios de pago en el mercado interior. Entró en vigor el 12 de enero de 2016 y los Estados miembros tuvieron hasta el 13 de enero de 2018 para transponerla a sus legislaciones nacionales**
ALCANCE	**1. Servicios de Pago:Regula todos los servicios de pago, incluyendo transferencias, pagos con tarjeta, y servicios de banca electrónica. 2. Proveedores de Servicios de Pago:Incluye tanto a los proveedores tradicionales (bancos) como a los nuevos actores del mercado, como los proveedores de servicios de iniciación de pagos (SIP) y los servicios de información sobre cuentas (SIC). 3. Usuarios de Servicios de Pago: Protege a los consumidores y empresas que utilizan servicios de pago, asegurando transparencia y seguridad en las transacciones. 4. Seguridad y Protección del Consumidor:Establece requisitos de seguridad, como la autenticación reforzada del cliente (SCA), para reducir el fraude en los pagos electrónicos**
ÓRGANO SUPERVISOR	**El organo supervisor es la Autoridad Bancaria Europea (EBA). La EBA es responsable de garantizar la aplicación coherente de la normativa de servicios de pago en toda la Unión Europea. Además, cada Estado miembro designa sus propias autoridades competentes para supervisar el cumplimiento de la PSD2 a nivel nacional.**
ESTADO	**Vigente**
Ámbito Subjetivo/Objetivo	**Busca fomentar un mercado de pagos más competitivo, seguro y transparente en la UE. Integración del mercado, Innovación y competencia y seguridad.**
Principales obligaciones	**1. Sistema de Concesión de Licencias:Las instituciones de pago, incluidas aquellas que ofrecen servicios de información sobre cuentas y de iniciación de pagos, deben obtener una licencia para operar. 2. Transparencia de Condiciones y Requisitos de Información:Los proveedores de servicios de pago deben ser transparentes sobre las condiciones y los gastos asociados a sus servicios. 3. Derechos y Obligaciones: Se establecen derechos y obligaciones claros tanto para los usuarios como para los proveedores de servicios de pago. 4. Requisitos de Seguridad: Se imponen requisitos estrictos de seguridad para los pagos electrónicos, incluyendo la autenticación reforzada del cliente (SCA), para reducir el riesgo de fraude. 5. Protección de Datos Financieros: Los proveedores deben garantizar la protección de los datos financieros de los consumidores.**
Normativa/ Framework de referencia	**Directiva 2002/65/CE:** Relativa a la comercialización a distancia de servicios financieros destinados a los consumidores **Directiva 2009/110/CE:** Sobre el acceso a la actividad de las entidades de dinero electrónico y la supervisión prudencial de dichas entidades **Directiva 2013/36/UE:** Relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión **Reglamento (UE) nº 1093/2010:** Por el que se crea la Autoridad Bancaria Europea

NORMA/ ESTÁNDAR	**Regulaciones del Banco Central Europeo**
ALCANCE	**Europa**
ÓRGANO SUPERVISOR	**Banco Central Europeo**
ESTADO	**Vigente**
Ámbito Subjetivo/Objetivo	**Las Regulaciones del Banco Central Europeo se centran en la estabilidad financiera, la política macroprudencial y la regulación financiera dentro del Eurosistema y la zona del euro. Entre las principales regulaciones están: Reglamento (UE) 2021/379 del Banco Central Europeo de 22 de enero de 2021 relativo a las partidas del balance de entidades de crédito y del sector de las instituciones financieras monetarias (refundición); Reglamento (UE) 2025/1355 del Banco Central Europeo, de 2 de julio de 2025, sobre los requisitos de vigilancia de los sistemas de pago de importancia sistémica (BCE/2025/22) etc.**
Principales obligaciones	**Dentro de las obligaciones establecidas por las regulaciones del Banco Central Europeo, el Reglamento 2025/1355 dispone que el BCE debe regular y ejercer la supervisión prudencial para asegurar que las entidades financieras cuenten con marcos internos sólidos para la gestión de riesgos operativos, incluidos aquellos relacionados con las tecnologías de la información y las comunicaciones (TIC), con el fin de garantizar la estabilidad y seguridad del sistema financiero europeo.**
Normativa/ Framework de referencia	**Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero.**

NORMA/ ESTÁNDAR	**Basilea III - Marco Regulador Internacional para Bancos como respuesta a la crisis financiera de 2007-2009**
ALCANCE	**Europa**
ÓRGANO SUPERVISOR	**Comité de Supervisión de Basilea**
ESTADO	**Vigente, en el caso de la Unión Europea a través de CRR (Reglamento UE nº 575/2013) y actualmente CRR II (Reglamento UE nº 876/2019)**
Ámbito Subjetivo/Objetivo	**El ámbito subjetivo de Basilea III comprende principalmente a entidades bancarias y otras autoridades de supervisión bancaria a nivel internacional, nacional y europeo. La regulación no delimita estrictamente qué se entiende por "banco", dejando cierto margen a cada jurisdicción para definirlo, pero en general se aplica a todas las entidades de crédito consideradas significativas o relevantes para el sistema financiero, incluyendo grupos bancarios y sucursales internacionales.**
Principales obligaciones	**Los requerimientos de Basilea III constituyen mínimos aplicables a bancos con actividad internacional. Exige a los banco mantener mayores niveles de capital de alta calidad (capital CET1), aplicar ratios de apalancamiento liquidez estrictos (LCR, NSFR), mejorar la gestión de riesgos crediticios y de mercado, además de someterse a pruebas de resistencia (stress tests). También introduce colchones anticíclicos y de conservación de capital para absorber pérdidas.**
Normativa/ Framework de referencia	**Basilea I y Basilea II**

2. Telecomunicaciones

- **Ley 11/2022, de 28 de junio, General de Telecomunicaciones.**
- **Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.**

NORMA/ ESTÁNDAR	**Ley 11/2022, de 28 de junio, General de Telecomunicaciones.**
ÁMBITO DE APLICACIÓN	Nacional
ALCANCE	Telecomunicaciones (instalación y explotación de las redes de comunicaciones electrónicas, la prestación de los servicios de comunicaciones electrónicas, sus recursos y servicios asociados, los equipos radioeléctricos y los equipos terminales de telecomunicación)
ÓRGANO SUPERVISOR	Ministerio de Asuntos Económicos y Transformación Digital; Comisión Nacional de los Mercados y la Competencia.
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	Aborda, de forma integral, el régimen de las «telecomunicaciones». Mediante esta Ley se procede a la transposición en España del Código Europeo de las Comunicaciones Electrónicas. Tiene como objetivo a corto plazo el apoyar la recuperación de la economía española tras la crisis sanitaria, impulsar a medio plazo un proceso de transformación estructural y lograr a largo plazo un desarrollo más sostenible y resiliente desde el punto de vista económico financiero. Excluye expresamente de su regulación los contenidos difundidos a través de servicios de comunicación audiovisual.
Principales obligaciones	Establece que la habilitación para instalar y explotar redes o prestar servicios en régimen de libre competencia, viene concedida con carácter general e inmediato por la ley, con el único requisito de notificación al Registro de operadores, dependiente de la Comisión Nacional de los Mercados y la Competencia. Obliga a las Administraciones públicas a que el planeamiento urbanístico prevea la necesaria dotación de infraestructuras de telecomunicaciones y garantiza el derecho de acceso de los operadores a infraestructuras de Administraciones públicas y a infraestructuras lineales Recoge las obligaciones de servicio universal y las relacionadas con la integridad y seguridad de las redes, así como los derechos de los usuarios de las telecomunicaciones y las garantías de acceso a las comunicaciones de emergencia y al número 112, de emergencias de ámbito europeo. Se regulan los requisitos esenciales que han de cumplir los equipos de telecomunicación, la evaluación de su conformidad con dichos requisitos y la vigilancia del mercado. Introduce como objetivo del uso del espectro lograr la cobertura del territorio nacional y de la población y de los corredores nacionales y europeos, así como la previsibilidad para favorecer inversiones a largo plazo. Regula la interoperabilidad de receptores de servicios de comunicación audiovisual radiofónicos para automóviles, de receptores de servicios de radio de consumo y equipos de consumo utilizados para la televisión digital, la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación o la coordinación de las ayudas públicas a la banda ancha y al desarrollo de la economía y empleo digitales y nuevos servicios digitales.
Normativa/ Framework de referencia	Ley 9/2014, de 9 de mayo, General de Telecomunicaciones Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones Real Decreto 2296/2004, de 10 de diciembre, por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y protección de los usuarios

NORMA/ ESTÁNDAR	**Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones**
ÁMBITO DE APLICACIÓN	Nacional
ALCANCE	Regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.
ÓRGANO SUPERVISOR	Agencia Española de Protección de Datos
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	Establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos y relativos a las comunicaciones que se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet, con el fin de posibilitar que dispongan de ellos los agentes facultados los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.
Principales obligaciones	Datos que deben conservarse: origen y destino de la comunicación, así como fecha, hora y duración; tipo de comunicación; equipo de comunicación o lo que se considera como equipo de comunicación; y localización del equipo de comunicación móvil. Duración de la conservación: Doce meses, si bien se podría ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, mediante reglamento. Acceso a los datos: El acceso a los datos conservados está restringido a las autoridades competentes y solo puede realizarse en el marco de investigaciones judiciales o en situaciones de emergencia, con la correspondiente autorización judicial. Protección de la privacidad: La Ley establece que la conservación de los datos debe realizarse respetando los derechos fundamentales de los ciudadanos, en especial la protección de su privacidad y el derecho a la protección de datos personales. Responsabilidad de los proveedores: Los proveedores de servicios de comunicaciones electrónicas tienen la obligación de almacenar y proteger los datos, y de garantizar que solo se acceda a ellos en las circunstancias legalmente permitidas.
Normativa/ Framework de referencia	Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. 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 (Reglamento general de protección de datos) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Ley 11/2022, de 28 de junio, General de Telecomunicaciones. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

3. Redes

- **Directiva (UE) 2016/1148 tambien conocida como Directiva NIS (Network and Information Systems)**
- **Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.**
- **Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.**
- **Real Decreto-Ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación**

NORMA/ ESTÁN-DAR	**La Directiva (UE) 2016/1148 tambien conocida como Directiva NIS (Network and Information Systems), tiene como objetivo garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea**
ALCANCE	Europeo. Operadores de Servicios Esenciales: Empresas que operan en sectores críticos como energía, transporte, salud, y agua. Proveedores de Servicios Digitales: Empresas que ofrecen servicios en línea, como motores de búsqueda, servicios de computación en la nube, y mercados en línea.
ÓRGANO SUPERVISOR	El órgano supervisor de la Directiva (UE) 2016/1148 es la Agencia de la Unión Europea para la Ciberseguridad (ENISA). Además, cada Estado miembro designa sus propias autoridades competentes para supervisar el cumplimiento de la directiva a nivel nacional
ESTADO	La Directiva (UE) 2016/1148 (Directiva NIS), fue derogada el 17 de octubre de 2024 y reemplazada por la Directiva (UE) 2022/2555 (NIS2).
Ámbito Subjetivo/Objetivo	1. Mejorar la Seguridad de las Redes y Sistemas de Información: Establecer requisitos mínimos comunes para la seguridad de las redes y sistemas de información. 2. Desarrollo de Capacidades y Planificación: Fomentar el desarrollo de capacidades y la planificación en los Estados miembros para enfrentar incidentes de seguridad. 3. Cooperación y Intercambio de Información: Facilitar la cooperación y el intercambio de información entre los Estados miembros y con la Agencia de la Unión Europea para la Ciber-seguridad (ENISA)
Principales obligaciones	1. Designación de Autoridades Competentes: Cada Estado miembro debe designar una o más autoridades nacionales competentes para supervisar la aplicación de la directiva. 2. Creación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT): Los Estados miembros deben establecer equipos de respuesta a incidentes de seguridad informática para gestionar y responder a los incidentes de ciberseguridad. 3. Estrategias Nacionales de Ciberseguridad: Los Estados miembros deben adoptar estrategias nacionales de ciberseguridad que incluyan objetivos y medidas adecuadas para alcanzar un alto nivel de seguridad de las redes y sistemas de información. 4. Identificación de Operadores de Servicios Esenciales: Los Estados miembros deben identificar a los operadores de servicios esenciales en sectores críticos como energía, transporte, salud, y agua, y asegurar que cumplan con los requisitos de seguridad. 5. Requisitos de Seguridad y Notificación de Incidentes: Los operadores de servicios esenciales y los proveedores de servicios digitales deben implementar medidas de seguridad adecuadas y notificar a las autoridades competentes sobre cualquier incidente que tenga un impacto significativo en la continuidad de los servicios
Normativa/ Framework de referencia	Tratado de Funcionamiento de la Unión Europea (TFUE): La directiva se fundamenta en el artículo 114 del TFUE, que trata sobre la armonización de las legislaciones de los Estados miembros para el correcto funcionamiento del mercado interior. Propuesta de la Comisión Europea: La Comisión Europea presentó la propuesta inicial de la directiva, que luego fue debatida y aprobada por el Parlamento Europeo y el Consejo. Dictamen del Comité Económico y Social Europeo: El Comité Económico y Social Europeo emitió un dictamen sobre la propuesta de la directiva, contribuyendo al proceso legislativo. Foro Europeo de Estados Miembros: La directiva se basa en los avances logrados en el Foro Europeo de Estados Miembros, que promovió discusiones y el intercambio de buenas prácticas en políticas de ciberseguridad.

NORMA/ ESTÁN-DAR	**Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.**
ALCANCE	Nacional
ÓRGANO SUPERVISOR	Para los operadores esenciales: En el caso de que también sean designados como operadores críticos será la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC). En el caso de que no sean operadores críticos: la autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente. ara los proveedores de servicios digitales: la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital. Para los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público: el Ministerio de Defensa, a través del Centro Criptológico Nacional.
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	Se encarga de regular la seguridad de las redes y sistemas de información utilizados para la provisión de servicios esenciales y servicios digitales en España. Este real decreto-ley se aplicará a la prestación de: *Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. *Los servicios digitales, considerados conforme se determina en el artículo 3 e), que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube. Igualmente, estarán sometidos a este real decreto-ley: *Los operadores de servicios esenciales establecidos en España. Se entenderá que un operador de servicios esenciales está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades. Asimismo, este real decreto-ley será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España. *Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
Principales obligaciones	*Las entidades que presten servicios esenciales o servicios digitales deben hacer evaluaciones previas de riesgos y adoptar medidas adecuadas para gestionar riesgos vinculados a la seguridad de las redes y sistemas de información que utilizan. *Están obligadas a notificar incidentes de seguridad a la autoridad competente. *Establece obligaciones específicas para operadores de servicios esenciales y proveedores de servicios digitales, incluyendo la supervisión y control por parte de las autoridades. *Favorece la cooperación entre autoridades públicas nacionales y europeas para gestionar adecuadamente la seguridad y los incidentes.
Normativa/ Framework de referencia	Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, (Directiva NIS)

NORMA/ ESTÁNDAR	**Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.** **El Real Decreto-ley 12/2018 de 7 de septiembre es la trasposición al ordenamiento jurídico español de la Directiva de la UE 2016/1148 (conocida como Directiva NIS) cuyo objeto es establecer mecanismos que, con una perspectiva integral, permitan mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, facilitando la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea**
ALCANCE	España. Desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Desarrolla esta disposición y define, entre otras cuestiones, la cooperación y coordinación de los CSIRT de referencia: CCN-CERT, MCCE e INCIBE-CERT, así como las tareas y apoyo de los CSIRT de referencia a los operadores críticos, operadores de servicios esenciales, proveedores de servicios digitales, las autoridades competentes, la Oficina de Coordinación de Ciberseguridad, entre otros. Esta legislación aplica a las empresas privadas que sean designadas operadores de servicios esenciales o consideradas proveedores de servicios digitales, con las consideraciones que en cada caso recoge este Real Decreto-ley. Estarán sometidos a este real decreto: a) Los operadores de servicios esenciales establecidos en España b) Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea
ÓRGANO SUPERVISOR	Las autoridades competentes en materia de seguridad de las redes y sistemas de información serán, con carácter general, las establecidas en el artículo 9.1 del Real Decreto-ley 12/2018, de 7 de septiembre. En particular, son autoridades competentes para los operadores de servicios esenciales que no sean operadores críticos de acuerdo con la Ley 8/2011, de 28 de abril, y que no estén incluidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, las siguientes: **a) Respecto al sector del transporte:** el Ministerio de Transportes, Movilidad y Agenda Urbana, a través de la Secretaría de Estado de Transportes, Movilidad y Agenda Urbana. **b) Respecto al sector de la energía:** el Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía. **c) Respecto al sector de las tecnologías de la información y las telecomunicaciones:** el Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales. **d) Respecto al sector del sistema financiero:** 1. El Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Economía y Apoyo a la Empresa, en el ámbito de los seguros y fondos de pensiones. 2. El Banco de España, para las entidades de crédito. 3. La Comisión Nacional del Mercado de Valores, para las entidades que prestan servicios de inversión y las sociedades gestoras de instituciones de inversión colectiva. **e) Respecto al sector del espacio:** el Ministerio de Defensa, a través de la Secretaría de Estado de Defensa. **f) Respecto al sector de la industria química:** el Ministerio de Interior, a través de la Secretaría de Estado de Seguridad. **g) Respecto al sector de las instalaciones de investigación:** el Ministerio de Ciencia e Innovación, a través de la Secretaría General de Investigación. **h) Respecto al sector de la salud:** el Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad. **i) Respecto al sector del agua:** el Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Medio Ambiente. **j) Respecto al sector de la alimentación:** 1. El Ministerio de Agricultura, Pesca y Alimentación, a través de la Secretaría General de Agricultura y Alimentación. 2. El Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad. 3. El Ministerio de Industria, Comercio y Turismo, a través de la Secretaría de Estado de Comercio. 4. El Ministerio de Consumo, a través de la Agencia Española de Seguridad Alimentaria y Nutrición (AESAN). **k) Respecto al sector de la industria nuclear:** 1. El Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía. 2. El Consejo de Seguridad Nuclear.
ESTADO	Vigente

Ámbito Subjetivo/Objetivo	En el ámbito europeo, con el objetivo de dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información, se aprobó la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como la Directiva NIS (Security of Network and Information Systems). Esta norma parte de un enfoque global de la seguridad de las redes y sistemas de información en la Unión Europea, integrando requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales. La transposición de la citada Directiva NIS al ordenamiento jurídico español se llevó a cabo mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Esta norma legal regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales, estableciendo mecanismos que, con una perspectiva integral, permiten mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, y fijando un marco institucional de cooperación que facilita la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea. El Real Decreto-ley 12/2018, de 7 de septiembre, habilita al Gobierno, en su disposición final tercera, para su desarrollo reglamentario. Con esa cobertura legal, y en cumplimiento del citado mandato y lo previsto en sus artículos 9.1 a), 11.1 a), 11.2, 16.2, 16.3, 19.1 y 19.5, el real decreto tiene 43/2021 tiene por finalidad desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información al cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales y a la gestión de incidentes de seguridad.
Principales obligaciones	* **Definición de una medidas técnicas y organizativas para la adecuada gestión de los riesgos de ciberseguridad:** Dichas medidas, que en términos del Real Decreto deberán relacionarse en la denominada Declaración de Aplicabilidad de medidas de seguridad, incluirán unas políticas de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas. La propia norma establece que dichas políticas deberán tratar los aspectos claves en seguridad, incluyendo -entre otros- el análisis y gestión de riesgos (incluyendo los de terceros o proveedores), inclusión del listado de medidas de seguridad, organizativas, tecnológicas y físicas, los planes de recuperación y aseguramiento de la continuidad de las operaciones, o la interconexión de sistemas. * **Designación de un responsable de seguridad:** éste podrá ser una persona, unidad u órgano colegiado que dentro de la compañía en cuestión actuará como responsable de la seguridad de la información, además de punto de contacto y coordinación con la autoridad competente. En este sentido, se establece que, entre otras funciones, el responsable de seguridad deberá: - Elaborar y proponer para aprobación las políticas de seguridad, así como la correspondiente Declaración de Aplicabilidad; - Supervisar y desarrollar la aplicación de las medidas técnicas y organizativas definidas en las citadas políticas de seguridad; - Remitir a la autoridad competente las notificaciones de incidentes; o supervisar la aplicación de las instrucciones y guías emanadas de la autoridad competente. * **Notificación y gestión de incidentes de seguridad:** El Real Decreto establece una obligación general de notificación a la autoridad competente aquellos incidentes que puedan tener “efectos perturbadores significativos” en los servicios que preste el operador en cuestión o que, atendiendo a su nivel de peligrosidad, puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, incluso si no han tenido un efecto relevante en las actividades del operador.
Normativa/ Framework de referencia	* Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. * DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

NORMA/ ESTÁN-DAR	**Real Decreto-Ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación**
ALCANCE	Nacional
ÓRGANO SUPERVISOR	Ministerio de Asuntos Económicos y Transformación Digital, a través del Centro de Operaciones de Seguridad 5G
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	Se encarga de regular la seguridad de las redes y sistemas de información utilizados para la provisión de servicios esenciales y servicios digitales en España. Este real decreto-ley se aplicará a la prestación de: *Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. *Los servicios digitales, considerados conforme se determina en el artículo 3 e), que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube. Igualmente, estarán sometidos a este real decreto-ley: *Los operadores de servicios esenciales establecidos en España. Se entenderá que un operador de servicios esenciales está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades. Asimismo, este real decreto-ley será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España. *Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
Principales obligaciones	*Las entidades que presten servicios esenciales o servicios digitales deben hacer evaluaciones previas de riesgos y adoptar medidas adecuadas para gestionar riesgos vinculados a la seguridad de las redes y sistemas de información que utilizan. *Están obligadas a notificar incidentes de seguridad a la autoridad competente. *Establece obligaciones específicas para operadores de servicios esenciales y proveedores de servicios digitales, incluyendo la supervisión y control por parte de las autoridades. *Favorece la cooperación entre autoridades públicas nacionales y europeas para gestionar adecuadamente la seguridad y los incidentes.
Normativa/ Framework de referencia	Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, (Directiva NIS)

Transversales

1. Comercio electrónico
2. Estándares y certificaciones

1. Comercio electrónico

- **Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.**

NORMA/ ESTÁNDAR	**Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.**
ALCANCE	Nacional. Aplica a los servicios de la sociedad de la información de carácter oneroso, pero también a los que no recibiendo contraprestación por parte del destinatario de los mismos, representan una actividad económica para su prestador; y a los prestadores de estos servicios.
ÓRGANO SUPERVISOR	Ministerio para la Transformación Digital y de la Función Pública, Secretaría de Estado de Digitalización e Inteligencia Artificial, Coordinador de Servicios Digitales (Comisión Nacional del los Mercados y la Competencia), Agencia Española de Protección de Datos Personales, Órganos que en el ejercicio de sus competencias para la protección del orden público, investigación penal, seguridad pública, defensa nacionañ salud, respecto a la dignidad y no discriminación, protección de la juventud y de la infancia, salvaguarda de derechos de propiedad intelectual, dicten resoluciones para interrupir la prestación del ser o para retirar los datos que los vulneran, respecto de los incumplimientos de estas resoluciones.
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	La LSSICE pretende equilibrar el desarrollo del comercio electrónico con la protección de los derechos de los usuarios, empresas y demás actores involucrados en el entorno digital, garantizar la seguridad jurídicay transparencia en las comunicaciones electrónicas; regulas las actividades comerciales electrónicas; proteger a consumidores y usuarios; promover el desarrollo de la sociedad de la información; establecer las responsabilidades de los prestadores de servicios; prevenir actividades ilícitas en el entorno digital y adecuar el marco jurídico español al marco regulatorio europeo sobre comercio electrónico. **Ambito subjetivo:** prestadores de servicios de la sociedad de la información (artículos 2 y 3) - prestadores de servicios de la sociedad de la información establecidos, domiciliados en España o que no estándolo, ofrezcan sus servicios a través de un establecimiento permanente en España. - prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo si el destinatario de los servicios radica en España y los servicios se refieren a: (a) propiedad intelectual; (b) publicidad emitida por instituciones de inversión colectiva; (c) seguro directo en régimen de establecimiento libre prestación de servicios; (d) obligaciones derivadas de contratos con consumidores persona física; (e) régimen de elección de la legislación aplicable al contrato por los contratantes; o (f) licitud de las comunicaciones comerciales por medios electrónicos no solicitadas. **Ámbito Objetivo:** servicios de la sociedad de la información (Anexo Definiciones) - servicios prestados a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario (Por ejemplo: contratación de bienes o servicios por vía electrónica; organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales; gestión de compras en la red por grupos de personas; etc) - servicios no remunerados por sus destinatarios, cuando sean una actividad económica para el prestador de servicios (Por ejemplo: envío de comunicaciones comerciales, suministro de información por vía telemática, etc.)

Principales obligaciones	- Identificar e informar de la identidad y datos de contacto del prestador de servicios de la sociedad de la información. - Informar de forma clara y precisa sobre los productos y servicios ofrecidos, precios (impuestos incluidos, y gastos de envío. - Publicar de forma comprensible y fácilmente accesible, las condiciones generales de contratación en los servicios ofrecidos por medios electrónicos. - Proporcionar al usuario una copia del contrato o las condiciones aceptadas. - Confirmar al usuario la recepción de pedidos o solicitudes realizadas electrónicamente. - Obtener el consentimiento expreso e informado de los destinatarios para el envío de comunicaciones comerciales con fines publicitarios, y establecer mecanosmos sencillos y electrónicos que permitan al destinatario darse de baja de dichas comunicaciones de forma sencilla y por medios electrónicos. - Identificar e imnplementar medidas de seguridad técnicas y organizativas, suficientes y adecuadas para proteger la seguridad de los datos y servicios ofrecidos - Cumplir con los requerimientos de la normativa de protección de datos personales vigente (RGPD y LOPDGDD) - Informar sobre el uso de cookies y dispositivos de seguimiento similares, y obtener el consentimiento expreso del usuario antes de instalarlas. - Informar de forma clara si se incluyen enlaces a otros sitios web y deslindar responsabilidades si es necesario. - Evitar prácticas como el spam, la publicidad engañosa o cualquier forma de fraude en línea.
Normativa/ Framework de referencia	Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). Directiva 98/27/CE del Parlamento Europeo y del Consejo de 19 de mayo de 1998 relativa a las acciones de cesación en materia de protección de los intereses de los consumidores (derogada) Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación. Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. 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 (Reglamento de Servicios Digitales) Ley 11/2022, de 28 de junio, General de Telecomunicaciones. 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 (Reglamento general de protección de datos) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)

2. Estándares y certificaciones

- **ISO 31000:2018 - Gestión de Riesgos**

- **ISO 37000:2021: Gobernanza de las organizaciones. Orientación**
  ISO 37002:2021: Sistema de gestión de la denuncia de irregularidades (Whistleblowing). Directrices
  ISO 37005:2024: Gobernanza de las organizaciones. Selección, creación y uso de indicadores. Orientación para los órganos de gobierno
  ISO 37006: Indicadores para una gobernanza de las organizaciones eficaz.
  ISO 37007: Directrices para la medición de la eficiencia

- **UNE-EN ISO/IEC 27001:2023 - Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. (ISO/IEC 27001:2022**

- **ISA/IEC / 62443 - Cybersecurity for Industrial Automation & Control Systems (IACS)**

- **UNE-EN ISO/IEC 15408-2:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Criterios de evaluación para la seguridad de TI. Parte 2: Componentes funcionales de seguridad (ISO/IEC 15408-2:2022)**

- **Public Company Accounting Reform and Investor Protection Act of 2002. Comúnmenete referida como la ley SOX.**

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

NORMA/ ESTÁNDAR	**ISO 31000:2018 - Gestión de Riesgos**
ALCANCE	Internacional. Se trata de una norma no certificable de gestión de riesgos, que proporciona directrices de buenas prácticas.
ÓRGANO SUPERVISOR	No hay un orgáno de supervisión específico
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	Cualquier organización que quiera integrar el enfoque de gestión de riesgos a nivel estratégico y operativo. Establece una serie de principios: *Integración: La gestión de riesgos debe integrarse en todos los niveles de la organización y en todos los procesos. *Estructurada: La gestión de riesgos debe tener un enfoque estructurado en la gobernanza de la organización. *Personalización: La gestión de riesgos debe adaptarse a las necesidades y características específicas de cada organización. *Inclusión: Todos los interesados relevantes deben participar en el proceso de gestión de riesgos. *Dinamismo: La gestión de riesgos debe ser proactiva y capaz de adaptarse a cambios en el entorno interno y externo. *Mejora continua: La organización debe buscar constantemente oportunidades para mejorar su enfoque de gestión de riesgos. *Basada en la información: La toma de decisiones en la gestión de riesgos debe basarse en información precisa y actualizada. *Factores humanos y culturales: El comportamiento humano y la cultura influyen en la gestión de riesgos.
Principales obligaciones	*Integración de la gestión de riesgos en todos los niveles y procesos de la organización, asegurando que la gestión del riesgo forme parte de la toma de decisiones y de la cultura organizacional. *La alta dirección debe definir políticas claras, asignar recursos, responsabilidades y asegurarse de que la gestión de riesgos esté alineada con los objetivos, la estrategia y la cultura de la organización. *Diseño del marco de gestión que incluye comprender el contexto interno y externo, asignar roles y responsabilidades, establecer comunicación efectiva y consulta con las partes interesadas, y asignar recursos adecuados. *Aplicar el proceso de gestión de riesgos que comprende la identificación, análisis, evaluación, tratamiento, monitoreo, revisión, comunicación y consulta de riesgos. *Cumplir con los principios básicos de gestión de riesgos, como ser sistemática, estructurada, basada en información precisa, inclusiva, dinámica, y orientada a la mejora continua. *Garantizar la transparencia y la rendición de cuentas mediante la documentación y el informe adecuado de los riesgos y las medidas adoptadas.
Normativa/ Framework de referencia	Es complementaria a la ISO 9001:2015 - Sistemas de Gestión de Calidad; ISO 31010:2019 – Técnicas de evaluación del riesgo; ISO 27001:2022 - Seguridad de la Información; ISO 22301:2019 - Continuidad del Negocio

NORMA/ ESTÁNDAR	**ISO 37000:2021: Gobernanza de las organizaciones. Orientación** **ISO 37002:2021: Sistema de gestión de la denuncia de irregularidades (Whistleblowing). Directrices** **ISO 37005:2024: Gobernanza de las organizaciones. Selección, creación y uso de indicadores. Orientación para los órganos de gobierno** **ISO 37006: Indicadores para una gobernanza de las organizaciones eficaz.** **ISO 37007: Directrices para la medición de la eficiencia**
ALCANCE	**Internacional. Si bien el estándar ISO 37000 no puede ser objeto de certificación como si de un sistema de gestión se tratase, la aplicación de sus directrices por parte de una organización sí puede verse sometida a evaluación externa.**
ÓRGANO SUPERVISOR	**No existe un órgano de supervisión específico**
ESTADO	**Vigente**
Ámbito Subjetivo/Objetivo	**La finalidad de la norma ISO 37000 es la de orientar a las empresas a conseguir los objetivos de una forma eficiente, generando un estado de confianza, transparencia y responsabilidad.**
Principales obligaciones	**La norma establece una serie de principios de gobernanza fundamentales, entre ellos:** ***Definir un propósito claro de la organización.** ***Establecer un modelo de generación de valor alineado con el propósito.** ***Dirigir y participar en la estrategia.** ***Supervisar el desempeño y comportamiento ético.** ***Asegurar rendición de cuentas y transparencia.** ***Promover la participación efectiva de las partes interesadas.** ***Liderazgo ético y competente.** ***Toma de decisiones basada en datos confiables.** ***Gobernanza de riesgos.** ***Responsabilidad social y sostenibilidad.** ***Garantizar la viabilidad y éxito a largo plazo.**
Normativa/ Framework de referencia	**Son complementarias: ISO 37301:2021 - Sistemas de Gestión del Cumplimiento; ISO 31000:2018 - Gestión del Riesgo**

NORMA/ ESTÁNDAR	**UNE-EN ISO/IEC 27001:2023 - Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. (ISO/IEC 27001:2022)** **Cabe reseñar que la familia de la ISO 27000 abarca casí un centenar de normas, siendo la mayoría un apoyo o complemento de la anterior en ámbitos específicos (como la 27701, en privacidad), como guías de implantación, TS (Technical Specification) o TR (Technical Report). Un listado más exhaustivo puede consultarse en** *https://www.iso.org/standard/iso-iec-27000-family* **o** *https://en.wikipedia.org/wiki/ISO/IEC_27000_family*
ALCANCE	**Normativa internacional multisectorial, aplicable en los sistemas que gestionan la seguridad de la información (ISMS o SGSI)**
ÓRGANO SUPERVISOR	**International Organization for Standardization (ISO, Internacional)** **International Electrotechnical Commission (IEC. Internacional)** **Comité Europeo de Normalización (CEN, Europa)** **Asociación Española de Normalización (UNE, España)**
ESTADO	**Vigente**
Ámbito Subjetivo/Objetivo	**UNE-EN ISO/IEC 27001: Establece los requisitos para establecer, implementar, mantener y mejorar un (ISMS o SGSI), su Anexo A (desarrollado en la 27002) recoge los objetivos de control y controles que deben ser seleccionados por las organizaciones para su implantación, cuando estos no se apliquen se deberá argumentar su no aplicablidad.** **Norma de carácter voluntario.**
Principales obligaciones	**- Definir los límites y el alcance del SGSI en la organización.** **- Establecer una Política y objetivos de seguridad de la información, que incluyan directrices y principios que regirán la seguridad de la información.** **- Evaluar los riesgos de seguridad de la información.** **- Tratar los riesgos de seguridad de la información, definiendo las acciones necesarias para tratarlos.** **- Detallar los controles que se aplicarán y justificar aquellos que no se implementen (Declaración de aplicabilidad o SOA)** **- Aplicar las medidas adecuadas en los controles, de acuerdo a los riesgos identificados.** **- Concienciar y formar al personal, así como validar su competencia.** **- Evidenciar el cumplimiento de las medidas aplicadas.**
Normativa/ Framework de referencia	**La ISO 27001 tiene su origen el la BS 7799-2002 del British Standards Institution (BSI), adoptada inicialmente como ISO/IEC17799. En la revisión del 2005 quedo incorporada como una nueva familia de normas catalogada como 27000, siendo su primera versión la ISO/IEC 27001:2005.**

NORMA/ ESTÁNDAR	ISA/IEC / 62443 - Cybersecurity for Industrial Automation & Control Systems (IACS) Es una serie de estándares internacionales donde se definen los requisitos y procesos para implementar y mantener sistemas de control y automatización industrial ciberseguros. Se puede consultar el listado completo en: https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards-by-topic
ALCANCE	Normativa internacional que establece un marco integral para la seguridad de los sistemas de automatización y control industrial en sectores como la energía, el agua y la industria química.
ÓRGANO SUPERVISOR	Sociedad Internacional de Automatización (ISA) Comisión Electrotécnica Internacional (IEC)
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	Proteger en los sectores industriales contra amenazas cibernéticas como ataques de malware, acceso no autorizado, interrupción del servicio y robo de información confidencial. Entre los ámbitos de aplicación están: automatización de edificios, generación y distribución de energía eléctrica, dispositivos médicos, transporte y las industrias de procesos (productos químicos, petróleo o gas). Norma de carácter voluntario.
Principales obligaciones	- Compromiso de la alta dirección - Evaluación de riesgos - Desarrollo de un plan de acción - Implementación de medidas de seguridad tales como el bastionado, la segmentación de redes, control de acceso, antimalware, registro de eventos, gestión de copias de seguridad e inventario de activos, entre otros. - Educación y concienciación
Normativa/ Framework de referencia	Originariamente constituida como Instrument Society of America, la International Society of Automation (ISA) es una organización fundada en 1945 y desde entonces ha venido desarrollando sus propios estándares dentro del mundo de automatización industrial.

NORMA/ ESTÁNDAR	UNE-EN ISO/IEC 15408-2:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Criterios de evaluación para la seguridad de TI. Parte 2: Componentes funcionales de seguridad (ISO/IEC 15408-2:2022) (Ratificada por la Asociación Española de Normalización en enero de 2024.)
ALCANCE	Normativa internacional multisectorial, aplicable a productos de tecnologías de la información (TI)
ÓRGANO SUPERVISOR	International Organization for Standardization (ISO, Internacional) International Electrotechnical Commission (IEC. Internacional) Comité Europeo de Normalización (CEN, Europa) Asociación Española de Normalización (UNE, España)
ESTADO	Vigente
Ámbito Subjetivo/Objetivo	Proporcionar y garantizar que el proceso de especificación, implementación y evaluación de productos de tecnologías de la información (TI) se ha llevado a cabo de manera rigurosa, estándar y repetible a un nivel adecuado para al uso al que está destinado. Con el objetivo de mejorar la disponibilidad, evitar la duplicidad de evaluaciones de seguridad y mejorar la eficiencia del proceso de evaluación de los productos TI y de los perfiles de evaluación. Norma de carácter voluntario.
Principales obligaciones	- Establecer unos objetivos y requisitos de las funciones de seguridad de un producto o sistema. - Realizar pruebas y estudios que verifiquen que los requisitos están definidos e implementados adecuadamente, y que el proceso de desarrollo y documentación de las funciones de seguridad cumple con lo establecido. -Establecer perfiles de protección
Normativa/ Framework de referencia	Common Criteria es el resultado de la unificación de tres estandares mundiales:Trusted Computer System Evaluation Criteria (TCSEC 1985, también conocido como Orange Book desarrollado por el Departamento de Defensa de los Estados Unidos), Information Technology Security Evaluation and Certification Scheme (ITSEC 1991, desarrollado por Francia, Alemania, los Países Bajos y el Reino Unido) y Canadian Trusted Computer Product Evaluation Criteria (CTCPEC 1993, derivado del TCSEC y desarrollado por Canada). En 1999 se convierte en la ISO/IEC 15408, desde la versión CC 2.1

NORMA/ ESTÁNDAR	**Public Company Accounting Reform and Investor Protection Act of 2002. Comúnmenete referida como la ley SOX.**
ÁMBITO DE APLICACIÓN	**Ámbito territorial: EE.UU.**
ALCANCE	**(i) Empresas públicas de EE.UU.** **(ii) Empresas extranjeras que coticen en la bolsa de EE.UU. O que emita valores que son ofrecidos públicamente en los EE.UU.** **(iii) en determinados supuestos, aplica a proveedores de servicios (i.e. auditoría, consultoría o tecnologías de la información) de las empresas sometidas a la ley.**
ÓRGANO SUPERVISOR	**Junta de Supervisión Contable de Empresas Públicas (PCAOB, por sus siglas en inglés)**
ESTADO	**En vigor desde el 30 de julio de 2002, con plazos de desarrollo e implementación de obligaciones.**
Ámbito Subjetivo/Objetivo	**Según el alcance establecido por la Ley Sarbanes-Oxley (SOX), se configura un régimen de responsabilidad personal directa, tanto penal como civil, para los principales responsables ejecutivos de la organización, concretamente el Chief Executive Officer (CEO) y el Chief Financial Officer (CFO). Asimismo, esta responsabilidad puede extenderse a otros actores clave en el sistema de control interno y supervisión, incluyendo a los miembros del Comité de Auditoría, los auditores externos, los directores y demás ejecutivos relevantes, quienes podrían enfrentar consecuencias legales en caso de incumplimiento normativo o de participación en prácticas fraudulentas.**
Principales obligaciones	**1. Certificación de los Estados Financieros /** Obligación: Los CEO y CFO deben certificar la exactitud de los informes financieros y que no contienen falsedades materiales. Sección: 302 **2. Controles Internos y Auditoría** / Obligación: Las empresas deben establecer y mantener controles internos efectivos para la preparación de los estados financieros y realizar una evaluación anual de su eficacia. Sección: 404 **3. Informe sobre Deficiencias en los Controles Internos** / Obligación: Las empresas deben divulgar cualquier deficiencia material en los controles internos y cualquier fraude que afecte a los empleados o los estados financieros. Sección: 404 **4. Protección de los Denunciantes (Whistleblowers)** / Obligación: Protección para los empleados que informen sobre fraudes o irregularidades dentro de la empresa. Sección: 1107 **5. Prohibición de Préstamos a Ejecutivos**/ Obligación: Prohibición de otorgar préstamos a ejecutivos y directores de la empresa. Sección: 402 **6. Auditoría Independiente** / Obligación: Las empresas deben contratar auditores externos independientes, y no pueden contratar a la misma firma para servicios no relacionados con auditoría. Sección: 201 **7. Revisión de la Auditoría por el PCAOB** / Obligación: Creación del Public Company Accounting Oversight Board (PCAOB) para supervisar la auditoría de las empresas públicas. Sección: 101 **8. Destrucción de Documentos /** Obligación: Prohibición de la destrucción, alteración o falsificación de registros contables o documentos relevantes para investigaciones o procedimientos judiciales. Sección: 802 **9. Responsabilidad Penal de los Ejecutivos** / Obligación: Los CEO y CFO enfrentan responsabilidad penal y sanciones si certifican informes financieros falsos. Sección: 906 **10. Regulación de los Conflictos de Intereses en la Auditoría** Obligación: Los auditores no pueden proporcionar ciertos servicios no relacionados con la auditoría a sus clientes, como consultoría financiera. Sección: 201 **11. Comité de Auditoría Independiente** / Obligación: Las empresas deben tener un comité de auditoría compuesto por miembros independientes del consejo de administración. Sección: 301 **12. Informe Financiero de las Empresas Extranjeras /** Obligación: Las empresas extranjeras que cotizan en EE. UU. deben cumplir con los mismos requisitos de auditoría y divulgación financiera que las empresas estadounidenses. Sección: 401 **13. Divulgación Rápida de Hechos Importantes** / Obligación: Las empresas deben divulgar rápidamente cualquier evento que pueda tener un impacto material en su situación financiera. Sección: 409

NORMA/ ESTÁNDAR	**Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.**
ALCANCE	**Nacional**
ÓRGANO SUPERVISOR	**Centro Criptológico Nacional (CCN)**
ESTADO	**Vigente**
Ámbito Subjetivo/Objetivo	**El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades del sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.** **También se aplica a los sistemas de información de las entidades del sector privado, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.**
Principales obligaciones	***Establece tres niveles de seguridad: bajo, medio y alto.** ***Gestión de la seguridad basada en los riesgos** *** Se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema** ***Establece como dimensiones de seguridad: Confidencialidad, integridad, disponibilidad, autencidad y trazabilidad** *** Auditoria cumplimiento ENS cada 2 años** *** Utilización de productos y servicios de seguridad certificados** ***Exige que las organizaciones clasifiquen la información que manejan según su nivel de sensibilidad**
Normativa/ Framework de referencia	ISO 27001:2022 - Seguridad de la Información Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

MAPA DE CYBERCOMPLIANCE

DATO

- RGPD
- LOPDGDD
- BCR
- DATA ACT

IA

- ISO IA
- AI ACT

SEGURIDAD DE LA INFORMACIÓN

RESILIENCIA

- REGLAMENTO DE SEGURIDAD
- CER

NIS2

- NIS2

INFRAESTRUCTURAS CRÍTICAS

- DORA
- CER
- LPIC
- REGLAMENTO PIC
- Contenidos mínimos PIC

SECTORIALES

BANCARIA

- Regulaciones BCE
- PCI - DSS
- BASILEA III
- PSD2

TELECOMUNICACIONES

- Ley 11/2022
- Ley 25/2007

REDES

- NIS1
- RD NIS
- RD-Ley Ciberseguridad 2018
- RD-Ley Seguridad 5G

TRANSVERSALES

ESTÁNDARES Y CERTIFICACIONES

- ISO 31000
- ISO 37000
- ISO 27000
- ISA/IEC 62443
- ISO/IEC 15408
- LEY SOX
- ENS

COMERCIO ELECTRÓNICO

- LSSI-CE

NACIONAL

EUROPA

INTERNACIONAL

Conclusiones

En definitiva, el presente Mapa de Cybercompliance en Seguridad de la Información se constituye como una **herramienta de referencia imprescindible para la interpretación, aplicación y despliegue operativo de los marcos regulatorios, estándares internacionales y buenas prácticas** que configuran el actual ecosistema normativo en materia de ciberseguridad y protección de la información.

La adecuada integración del cumplimiento normativo en los sistemas de gestión de riesgos y en la estrategia global de ciberseguridad forman, hoy más que nunca, un elemento diferenciador para la sostenibilidad, la resiliencia y la competitividad de las organizaciones, tanto en el sector público como en el privado.

Según los últimos datos publicados por el **Instituto Nacional de Ciberseguridad (INCIBE)**, en 2024 se gestionaron en España más de **97.000 incidentes de ciberseguridad**, lo que representa un incremento del **16,6%** respecto al ejercicio anterior. De estos, **341 incidentes afectaron a operadores esenciales e importantes conforme a la Directiva NIS2**, evidenciando la creciente presión regulatoria y operativa sobre los sectores críticos y la necesidad de reforzar la capacidad de respuesta y la resiliencia organizativa.

El ransomware y el fraude online continúan siendo las amenazas más frecuentes, mientras que la sofisticación de los ataques y la irrupción de nuevas tecnologías, como la inteligencia artificial, amplían la superficie de exposición y los vectores de riesgo.

Datos de 2024 del Instituto Nacional de Ciberseguridad:

97.000	**16,6%**	**341**
incidentes de ciberseguridad	**más que en 2023**	**operadores esenciales afectados**

El *informe sobre el Estado de la Ciberseguridad en la Unión Europea*, elaborado por **ENISA** y recogido por el **Departamento de Seguridad Nacional**, subraya que el nivel de amenaza en la UE se mantiene en un umbral sustancial, con una probabilidad significativa de que entidades críticas sean objetivo de ataques o sufran brechas a través de vulnerabilidades emergentes. Si bien España presenta un nivel de madurez elevado en materia normativa y dispone de instrumentos avanzados como el Esquema Nacional de Seguridad y la Estrategia Nacional de Ciberseguridad, persisten retos relevantes en la implementación homogénea de medidas, la gestión de la cadena de suministro y la capacitación de los órganos de gobierno y equipos operativos.

A pesar de los avances regulatorios y de la consolidación de organismos como el **CCN-CERT** y la **Oficina de Coordinación de Ciberseguridad del Ministerio del Interior**, solo una minoría de organizaciones españolas dispone de infraestructuras plenamente preparadas para mitigar ciberataques de gran envergadura.

Esta realidad pone de manifiesto la necesidad de seguir invirtiendo en capacidades, formación y cultura de ciberseguridad, así como en la adopción de modelos de gobierno alineados con los más altos estándares internacionales.

Desde ISMS Forum, reiteramos nuestro compromiso con la divulgación y actualización permanente de este compendio normativo, conscientes de la necesidad de anticipar los cambios regulatorios y de fomentar una cultura de cumplimiento proactiva, transversal y basada en el principio de mejora continua. Invitamos a los profesionales y responsables de seguridad a utilizar este mapa como base para la toma de decisiones informadas, la priorización de iniciativas y la consolidación de modelos de gobierno corporativo robustos y alineados con las mejores prácticas internacionales.

La evolución constante del entorno digital y la sofisticación de las amenazas exigen una vigilancia normativa permanente y una adaptación ágil de los marcos de cumplimiento. Solo mediante una gobernanza efectiva, una gestión integral del riesgo y una cultura organizacional orientada al cumplimiento será posible garantizar la protección de los activos críticos, la confianza de los usuarios y la continuidad de las operaciones en un contexto global cada vez más exigente.

Mapa de Cybercompliance en la seguridad de la información

Noviembre 2025

Website
www.ismsforum.es

Email
proyectos@ismsforum.es

Teléfono
(+34) 636 69 13 92