Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
ontsi
incibe_
Plan de Recuperación, Transformación y Resiliencia

análisis comparativo de la normativa y regulación sobre ciberseguridad

Edición 2025

Datos 2024

índice

Análisis comparativo de la normativa y regulación sobre ciberseguridad. Observatorio Nacional de Tecnología y Sociedad. Red.es. Secretaría de Estado de Digitalización e Inteligencia Artificial. Ministerio para la Transformación Digital y de la Función Pública. Reservados todos los derechos. La normativa a la que hace referencia este informe fue actualizada en marzo de 2026.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
red.es · ontsi · observa ciber · incibe_ · Plan de Recuperación, Transformación y Resiliencia

01
Resumen ejecutivo

El Ontsi publica el *Análisis comparativo de la Normativa y Regulación sobre Ciberseguridad*, una herramienta para comprender el marco regulatorio de la ciberseguridad y su interacción con la protección de datos en la Unión Europea y en España. En el informe se presenta el contexto y las amenazas emergentes, y subraya la necesidad de que entidades públicas y privadas se adapten a ellas. Para garantizar una línea base de seguridad, la UE y España han desarrollado un corpus normativo que fija medidas comunes.

El documento sistematiza el marco normativo y regulatorio de la ciberseguridad (principios estratégicos, directrices, objetivos, medidas y políticas) y armoniza disposiciones legales con la gestión efectiva de riesgos derivados del ciberespacio. Además, identifica los organismos públicos con competencias en ciberseguridad en España.

El estudio busca formar y concienciar sobre el marco normativo aplicable a la protección de sistemas, información y servicios, y facilitar el conocimiento de las autoridades y recursos disponibles.

En infraestructuras críticas, la normativa española y europea persigue la continuidad de los servicios esenciales o críticos, reforzando la capacidad de respuesta ante incidentes y exigiendo medidas técnicas y organizativas proporcionales al riesgo.

En conclusión, se constata una mayor alineación entre la normativa nacional y las disposiciones de la Unión Europea, y favorece la cooperación y armonización entre Estados miembros.

02
Introducción y contexto

Este capítulo expone un análisis comparativo de las principales normativas, regulaciones y estándares de ciberseguridad en España y en la Unión Europea. Integra marcos legales y estrategias, además de las novedades recientes en el entorno digital.

El objetivo es fijar directrices que permitan un uso seguro del ciberespacio. La visión integradora debe asegurar tanto el progreso como la protección frente a *ciberamenazas*[i] , con acciones coherentes de prevención, detección, defensa, respuesta y recuperación.

Contexto

La UE ha desarrollado un marco normativo para reforzar la ciberseguridad e implantar homogeneidad regulatoria entre estados. La **Estrategia de Ciberseguridad europea** tiene como propósito aumentar la resiliencia frente a las ciberamenazas y garantizar que la ciudadanía y las entidades utilicen las tecnologías digitales con un alto grado de fiabilidad. La estrategia, basada en los avances de marcos anteriores, formula propuestas concretas en tres ámbitos de actuación:

1. **Resiliencia, capacidad tecnológica y liderazgo.**
2. **Capacidad de prevención, detección y respuesta ante ciberataques.**
3. **Cooperación y fomento de normas internacionales.**

En el ámbito nacional, y en el marco de la Estrategia de Seguridad Nacional, se ha desarrollado la Estrategia Nacional de Ciberseguridad, que busca garantizar los intereses del país ante los riesgos que derivan de los ciberataques en el ciberespacio.

De acuerdo con el **artículo 10 de la Ley 36/2015**[1] , se consideran ámbitos de especial interés para la Seguridad Nacional aquellos que requieren atención específica por resultar básicos para preservar derechos y libertades, así como el bienestar de la ciudadanía y el suministro de servicios y recursos esenciales. Entre estos ámbitos se incluye expresamente la ciberseguridad.

Asimismo, el **artículo 7 de la Ley 36/2015** establece la necesidad de proteger las infraestructuras críticas digitales, prevenir los ciberataques y reforzar la cooperación entre el sector público y el privado.

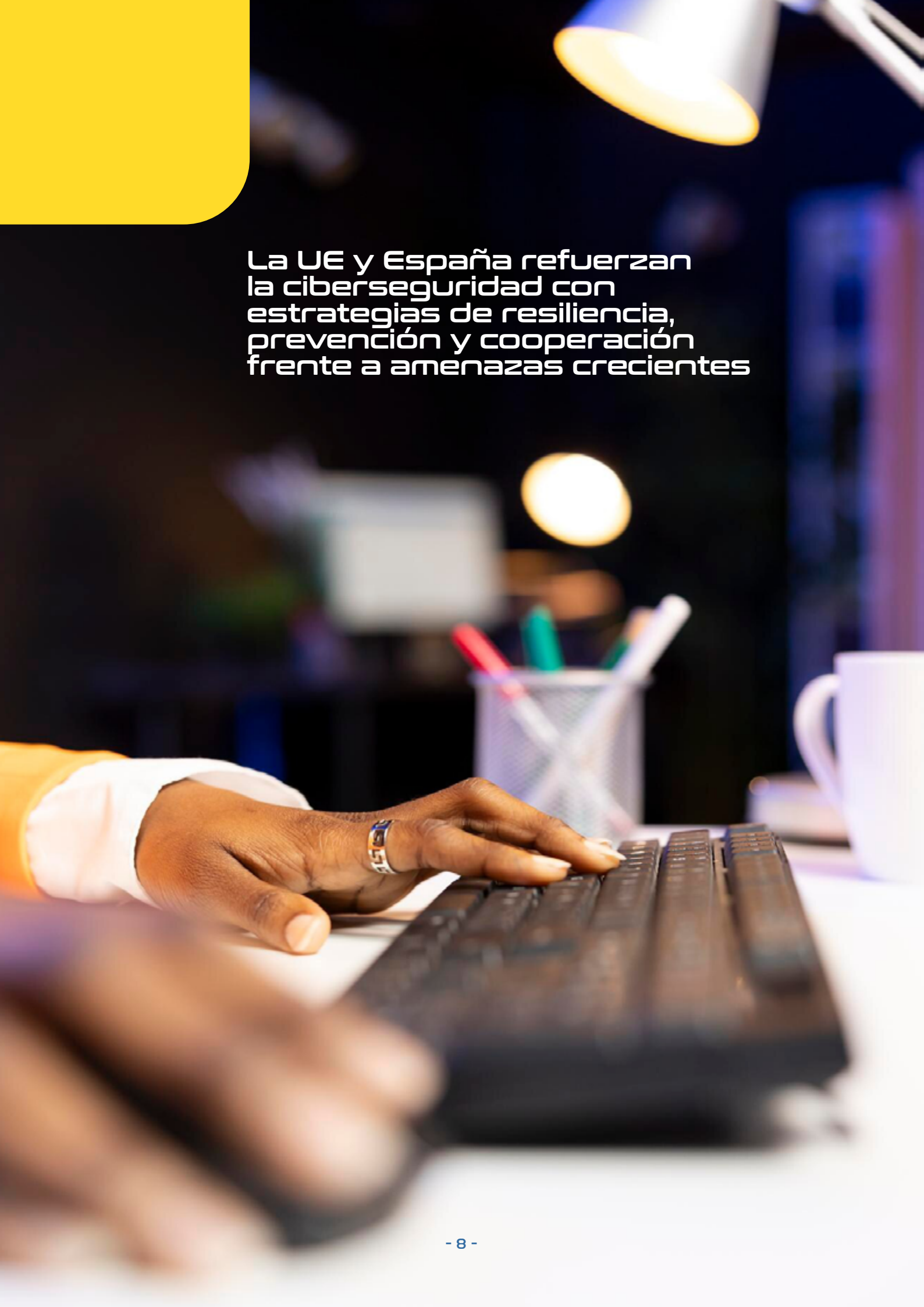
En esta misma línea, la **Orden PJC/522/2025**[2] , publicada en el BOE el 26 de mayo de 2025, oficializa el acuerdo del Consejo de Seguridad Nacional de 24 de abril de 2025. Dicho acuerdo aprueba el procedimiento para elaborar una nueva Estrategia Nacional de Ciberseguridad. El borrador final será presentado al Consejo Nacional de Ciberseguridad y, tras su aprobación, se elevará al Consejo de Seguridad Nacional para su adopción definitiva.

La implantación y desarrollo de estas regulaciones persiguen la uniformidad normativa para dar una respuesta eficaz a los incidentes que se producen en el ciberespacio, en especial en sectores estratégicos. La creciente dependencia tecnológica ha hecho que la cadena de suministro sea vulnerable a numerosos ciberataques que afectan tanto a organizaciones como a la sociedad.

[1] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

[2] Orden PJC/522/2025, de 23 de mayo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 24 de abril de 2025, por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia Nacional de Ciberseguridad.

La UE y España refuerzan la ciberseguridad con estrategias de resiliencia, prevención y cooperación frente a amenazas crecientes



Ante este escenario, la Unión Europea ha intensificado la aprobación de nuevas normas clave en los últimos años. Entre ellas, la **Directiva NIS2** amplía y refuerza las obligaciones impuestas a Estados miembros, instituciones públicas y entidades privadas.

En línea con la NIS2[3] , España ha iniciado la tramitación del **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad**, que adapta el ordenamiento jurídico español a esta Directiva y completa sus disposiciones[4].

Esta serie de normativas no solo persiguen la mejora en cuanto a la preparación y resiliencia ante los distintos ciberataques, sino que también llevan a cabo el impulso sobre las modificaciones estructurales en relación con la gestión de la seguridad digital. Tanto es así que se aboga por la inclusión de los CISOs en los órganos que llevan a cabo la toma de decisiones de la alta dirección, así como por la implantación de mecanismos de ámbito sancionador que protejan el cumplimiento de las medidas de seguridad.

En el plano sectorial, se han aprobado reglamentos concretos como **DORA**[5], que garantiza la continuidad del servicio en el sector financiero ante incidentes digitales, y la **Directiva CER**[6], la cual refuerza todas aquellas exigencias de seguridad en los servicios considerados esenciales. Con respecto a la transposición nacional de la Directiva CER, el 27 de mayo de 2025, el Consejo de Ministros aprueba el Anteproyecto de Ley de Protección y Resiliencia de las Entidades Críticas. Una vez aprobada definitivamente, esta norma traspondrá al ordenamiento jurídico español la Directiva (UE) 2022/2557[6].

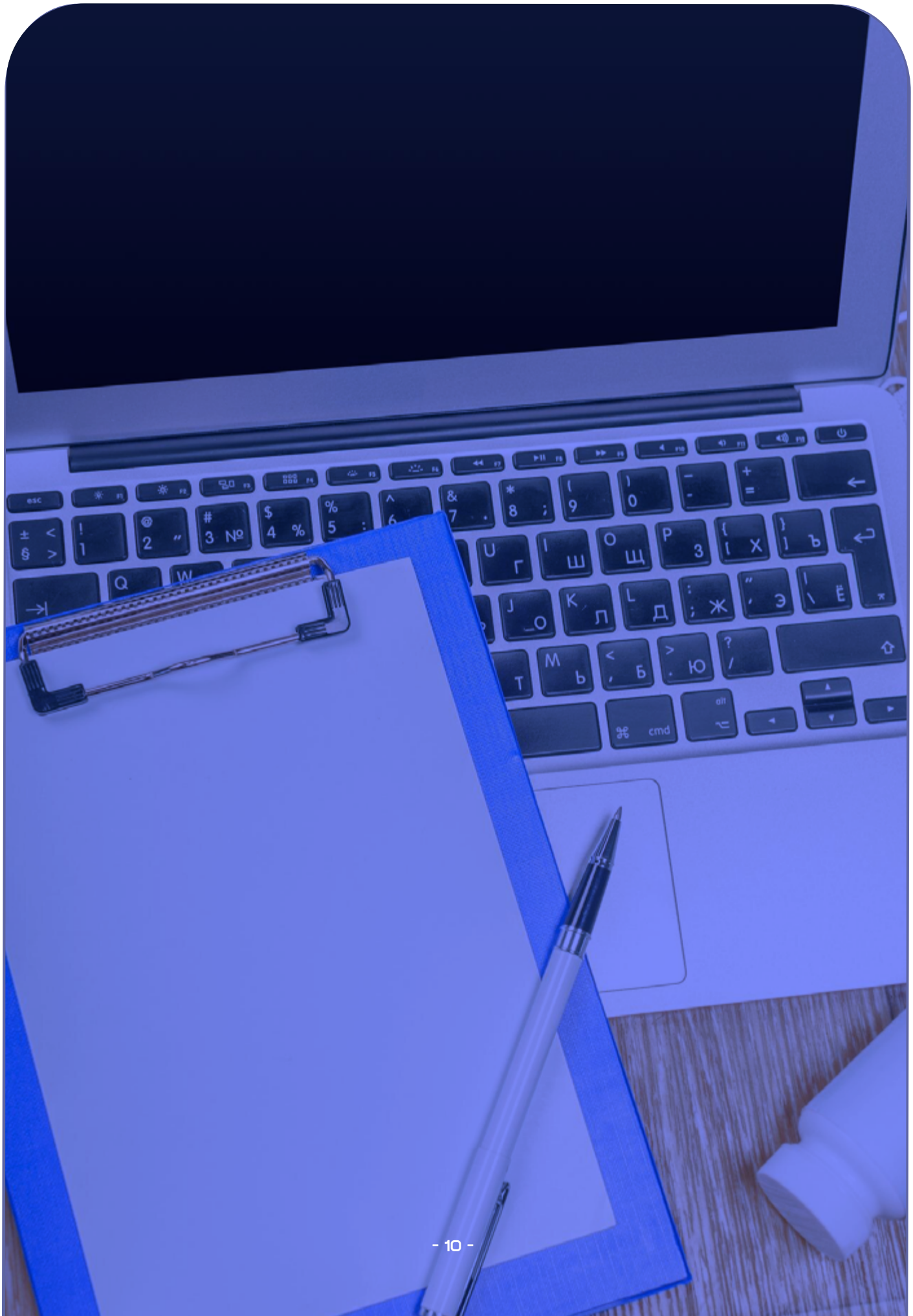
España tramita la ley de ciberseguridad que adapta la normativa a la Directiva NIS2

[3] 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 la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148 (Directiva NIS2).

[4] Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad a propuesta conjunta de los ministerios del Interior, de Defensa y para la Transformación Digital y de la Función Pública.

[5] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011 (Reglamento DORA).

[6] 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 (Directiva CER).



Por otra parte, también son relevantes las iniciativas como el **Reglamento sobre la Ciberseguridad**[7], que consolida la Agencia de Ciberseguridad de la Unión Europea, además de la creación de un sistema de certificación; y el **Reglamento de Ciberresiliencia**[8], que establece aquellos requisitos de seguridad de carácter obligatorio, para los productos tecnológicos.

En cuanto a la evaluación de los riesgos[ii], la Directiva NIS2 obliga a las organizaciones esenciales de la UE a implantar una gestión integral de riesgos en ciberseguridad:

Entre los aspectos principales figuran: la identificación de sistemas[iii], activos[iv] y vulnerabilidades[v]; la implantación de medidas técnicas y organizativas; la aplicación proactiva de procedimientos; y el cumplimiento normativo con su supervisión y régimen sancionador.

La interconexión del ciberespacio permite que los ciberataques afecten a cualquier país, organización o persona. Por ello, es esencial disponer de marcos normativos que identifiquen amenazas e incidentes y refuercen la cooperación internacional[9].

Enfoque metodológico

El informe se ha elaborado a partir de un enfoque estructurado que permite analizar la normativa y regulación en materia de ciberseguridad en España y en la Unión Europea. Para ello, se ha llevado a cabo un estudio basado en la recopilación de normativa, regulación e informes especializados.

Este enfoque combina:

- **Investigación documental, con un examen amplio de las normativas y regulaciones vigentes.**
- **Referencia comparativa, que contrasta marcos nacionales y europeos de ciberseguridad.**
- **Buenas prácticas, extraídas de las estrategias de ciberseguridad en ambos ámbitos.**

La investigación se centra en un análisis sistemático y a gran escala de documentos normativos relevantes. Con ello se definen capacidades, se identifican modelos de madurez y se facilita la comparación entre distintos sistemas.

En la parte final del informe, las referencias se organizan conforme a los bloques normativos descritos. Este orden responde a un criterio de coherencia y claridad en la lectura, y se presenta en secuencia cronológica para reforzar la comprensión.

[7] 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) nº 526/2013 (Reglamento sobre la Ciberseguridad).

[8] 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) nº 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia).

[9] CCN-CERT-IA-04-24_Ciberamenazas_y_Tendencias_2024

03
Estrategias en el ámbito de la ciberseguridad

Estrategia de seguridad nacional

El **Real Decreto 1150/2021, de 28 de diciembre**, aprueba la Estrategia de Seguridad Nacional de 2021. Se define como un instrumento legal fundamental que establece el marco político-estratégico de referencia de la política de Seguridad Nacional. El **Consejo de Seguridad Nacional** es el órgano responsable de su elaboración, con participación de los departamentos ministeriales y del **Centro Nacional de Inteligencia**.

La Estrategia de Seguridad Nacional 2021 se estructura en **cinco capítulos**:

Capítulo 1. **Seguridad global y vectores de transformación**. Aborda la incertidumbre ante un futuro condicionado por la transformación digital y la transición ecológica, principales palancas de cambio en un escenario de competencia geopolítica.

Capítulo 2. **Una España segura y resiliente**. Analiza el entorno geográfico de España (Europa, Magreb y Oriente Próximo, África Subsahariana, América del Norte, América Latina y el Caribe, y Asia-Pacífico) desde el prisma de la seguridad nacional.

Capítulo 3. **Riesgos y amenazas**. Incluye como novedad las campañas de desinformación, y considera la tecnología y las estrategias híbridas como elementos transversales.

Capítulo 4. **Planeamiento estratégico integrado.** Fija tres objetivos prioritarios: gestión de crisis, seguridad de capacidades tecnológicas y sectores estratégicos, y desarrollo de capacidades preventivas y de respuesta frente a estrategias híbridas.

Capítulo 5. **Gestión de crisis**. Plantea una visión progresiva desde la normalidad hasta la recuperación tras una situación crítica.

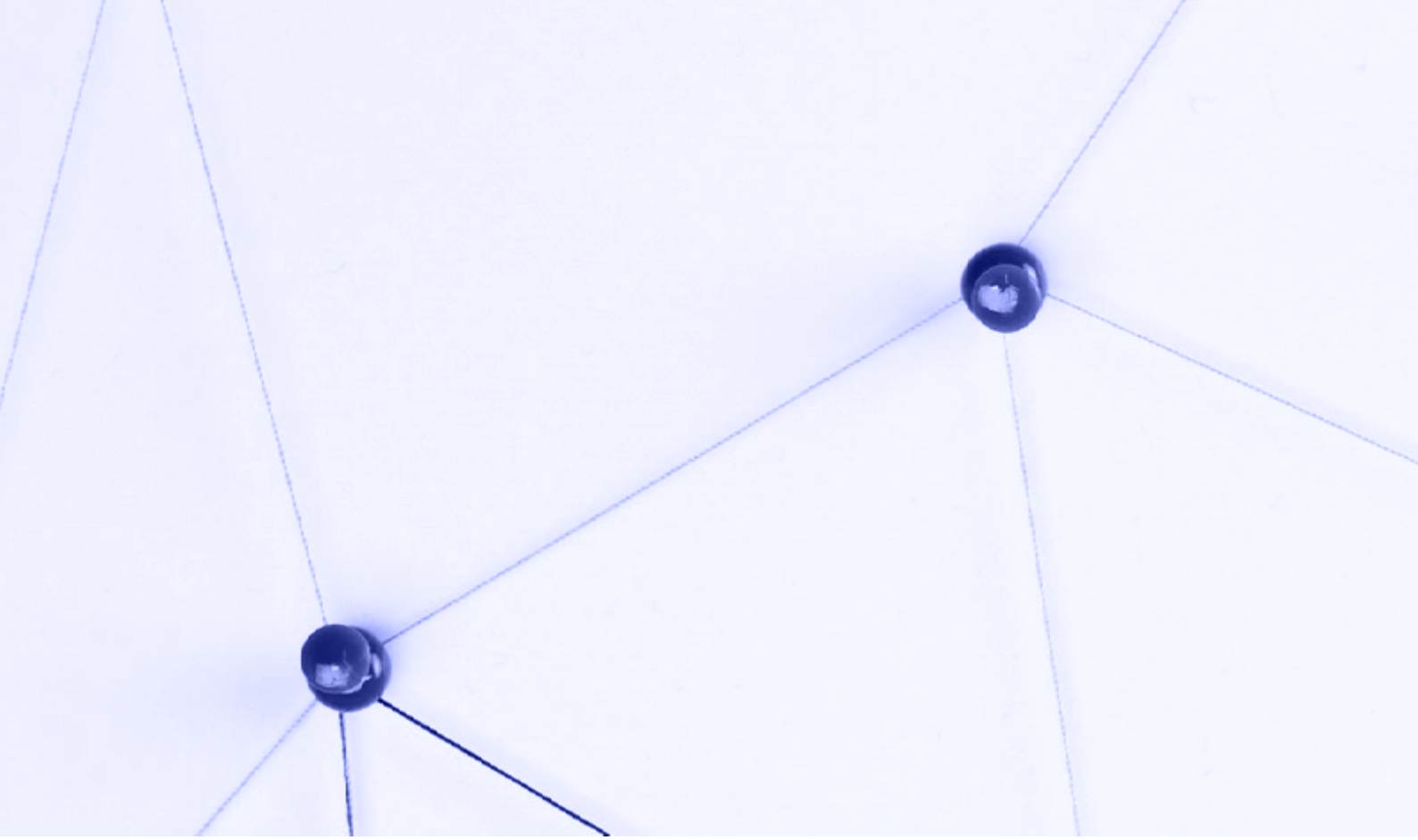
Entre las iniciativas destacadas figuran: la creación de una reserva estratégica de capacidades nacionales de producción industrial y el desarrollo de un plan integral de seguridad para Ceuta y Melilla.

En el plano internacional, España impulsa una mayor autonomía estratégica europea, en coordinación con la **Política Común de Seguridad y Defensa** y el **espacio de libertad, seguridad y justicia**. También fomenta la seguridad sanitaria, la unión energética y una mayor implicación de la Unión Europea en la gestión de crisis transfronterizas.

La estrategia plantea el dilema entre el repliegue estratégico de los Estados y la necesidad de cooperación e intercambio de información para respuestas conjuntas. En este contexto, se subraya la importancia de un sistema multilateral, universal y regional, capaz de responder de forma coordinada y efectiva.

Entre las principales medidas están:

- **Prevención y detección de amenazas:** Desarrollo de capacidades avanzadas para anticipar y detectar ciberataques y otras amenazas, mediante la inversión en tecnología, investigación e innovación.



- **Respuesta y recuperación:** Establecimiento de protocolos y mecanismos de respuesta rápida que faciliten la mitigación de incidentes y la recuperación de servicios, para garantizar la continuidad operativa.
- **Protección de Infraestructuras críticas:** Implementación de medidas específicas para asegurar la integridad[vi], disponibilidad[vii] y confidencialidad[viii] de los sistemas y redes que sostienen los servicios esenciales del Estado.
- **Coordinación y gobernanza:** Definición clara de roles y responsabilidades de los diferentes actores involucrados en la seguridad nacional, para asegurar una gestión coordinada y eficaz tanto a nivel interno como en cooperación con los aliados internacionales.

La estrategia enfatiza tres ejes:

- **Anticipación:** Creación de un sistema de alerta temprana y planes de gestión de crisis con participación de comunidades autónomas.
- **Integración:** Coordinación entre administraciones públicas, colaboración público-privada e implicación de la ciudadanía.
- **Resiliencia:** Potenciar la capacidad de resistencia, transformación y recuperación ante crisis.

Finalmente, subraya la necesidad de cadenas de suministro menos dependientes del exterior para contener crisis y fortalecer la resiliencia social y económica.

Reducir la dependencia exterior de las cadenas de suministro ayuda a contener mejor las crisis

Estrategia de ciberseguridad de la Unión Europea

La transformación digital ha incrementado el número y la complejidad de las amenazas en el ciberespacio. Ante esta situación, la UE debe impulsar iniciativas que garanticen una digitalización lo más segura posible, mediante normativas, estándares y buenas prácticas que protejan infraestructuras críticas y servicios esenciales, y que acompañen el desarrollo de tecnologías emergentes.

La estrategia de ciberseguridad de la UE determina qué recursos y herramientas deben aprovecharse y potenciarse para alcanzar una soberanía tecnológica en este ámbito. Asimismo, describe la manera en que la UE puede reforzar sus mecanismos de cooperación con agentes externos en materia de defensa del ciberespacio, a través de la Comisión Europea, el Servicio Europeo de Acción Exterior, la Agencia Europea de Defensa, la Agencia de la UE para la Ciberseguridad (ENISA) y la Agencia de la UE para la cooperación policial (Europol).

Esta soberanía tecnológica debe basarse en **cuatro pilares**:

1. **Mercado interior**
2. **Fuerzas y cuerpos de seguridad**
3. **Diplomacia**
4. **Defensa**

A partir de esta base, la UE debe responder conjuntamente ante los ciberataques que se originen, y así poder lograr una conciencia compartida de todo tipo de amenazas.

La estrategia tiene como objetivo principal garantizar un Internet global y abierto, con medidas sólidas de seguridad en los casos en los que existan riesgos para la seguridad o para los derechos y libertades de la ciudadanía.

Normativas y Regulaciones destacadas a nivel europeo

- **Directiva NIS2**[10]**:** Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión Europea.
- **Directiva CER**[11]**:** Tiene como objetivo garantizar las medidas de seguridad específicas para la prestación de los servicios esenciales en la totalidad de los Estados miembros de la UE.
- **Reglamento DORA**[12]**:** Implica al sector financiero, el reglamento tiene como finalidad principal la continuidad de los servicios financieros en todos aquellos casos en los que se produzcan ciberataques.
- **Reglamento sobre la Ciberseguridad**[13]**:** Se adopta en el año 2019, por el que se refuerza la importancia de la Agencia de la Unión Europea para la Ciberseguridad, y establece un marco de certificación en materia de ciberseguridad.
- **Reglamento de Ciberresiliencia**[13]**:** Es un acuerdo promulgado por la Unión Europea que promueve el respaldo hacia un mercado único digital seguro y protegido, e incluye requisitos en ciberseguridad de carácter obligatorio en relación con los productos de *software* y *hardware*.
- **Reglamento de Cibersolidaridad**[15]**:** Entra en vigor el 4 de febrero de 2025 con el objetivo de mejorar la prevención, detección y respuesta a los incidentes de ciberseguridad en toda la Unión Europea.

Asimismo, la **sensibilización** sobre la ciberseguridad es también uno de los aspectos relevantes a tratar dentro de la Estrategia de la UE, debido a las consecuencias que se pueden derivar de un uso accidental de las tecnologías. Por lo tanto, la Comisión Europea trata de formar y concienciar sobre la ciberseguridad y promueve las mejores prácticas entre la ciudadanía y personas usuarias de los Estados miembros.

Estrategia nacional de ciberseguridad

La **Estrategia nacional de Ciberseguridad de España** se publica en BOE el 30 de abril de 2019 y desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017. Tiene como objetivo garantizar la seguridad, infraestructuras y tecnologías que integran el ciberespacio.

El documento está estructurado en **cinco capítulos**:

1. **El ciberespacio, más allá de un espacio común global.**
2. **Las amenazas y desafíos en el ciberespacio.**
3. **Propósitos, principios y objetivos para la ciberseguridad.**
4. **Líneas de acción y medidas.**
5. **La ciberseguridad en el Sistema de Seguridad Nacional.**

Capítulo 1. Se analizan las oportunidades y desafíos que presenta el ciberespacio, al destacar que es un espacio global dinámico pero vulnerable. Se identifican cuatro ejes principales:

- **Oportunidades y desafíos:** El ciberespacio facilita la conectividad global y el desarrollo económico, pero a su vez genera vulnerabilidades y desafíos en la protección de datos y seguridad.
- **Infraestructura digital:** La seguridad depende de elementos físicos y lógicos como componentes, redes y sistemas de información. Las infraestructuras críticas comprometen la seguridad ya que están expuestas a posibles ciberataques y errores en el diseño de *hardware* y/o *software*.
- **Seguridad internacional:** Es importante garantizar un ciberespacio seguro y confiable, para ello España promueve la cooperación internacional en el ámbito de la ciberseguridad y participa con la UE, la OTAN o la ONU.
- **Nueva concepción del ciberespacio:** Es esencial promover una cultura de ciberseguridad en toda la sociedad. Además, la disuasión y ciberinteligencia se consideran dos elementos clave para anticiparse a determinadas amenazas.

Capítulo 2. Se evalúan las principales amenazas y desafíos del ciberespacio a los que se enfrenta España, y distingue entre aquellas que afectan a los activos del ciberespacio y elementos tecnológicos, y aquellas que emplean el ciberespacio para realizar actividades maliciosas.

Capítulo 3. Se establece el principal objetivo de la estrategia y los principios que la rigen. La Estrategia Nacional de Ciberseguridad se inspira en los siguientes cuatro principios rectores:

- **Unidad de Acción:** Refuerzo de la respuesta estatal mediante coherencia, coordinación y rapidez.
- **Anticipación:** Mecanismos de alerta y prevención en organismos especializados, con participación del sector privado.
- **Eficiencia:** Uso de sistemas tecnológicos avanzados y multipropósito, cuya sostenibilidad exige planificación y recursos.
- **Resiliencia:** Obligación del Estado de garantizar la disponibilidad de elementos esenciales y reforzar la protección de las redes de información y comunicaciones.

Además, se fijan cinco objetivos que orientan la acción del Estado en el ámbito de la ciberseguridad:

- Seguridad de las redes y sistemas de información y comunicaciones del sector público y servicios esenciales, al mejorar las capacidades de prevención, detección y respuesta ante incidentes.

- Uso seguro y fiable del ciberespacio frente a un uso malicioso, al garantizar la seguridad de los activos estratégicos.
- Proteger el ecosistema empresarial y social de la ciudadanía, al impulsar la ciberseguridad.
- Cultura y compromiso con la ciberseguridad, al tiempo que impulsa el desarrollo actividades de I+D+i, fortalece la industria y protege el patrimonio tecnológico y de la propiedad intelectual e industrial.
- Seguridad del ciberespacio en el ámbito internacional, lo que fortalece la seguridad y autonomía estratégica europea, así como la cooperación internacional bilateral en materia de ciberseguridad.

Capítulo 4. Se establecen las siete líneas de acción dirigidas a la consecución de los objetivos. Dos para los objetivos uno y cuatro y una para los otros tres:

- Reforzar las capacidades frente a amenazas.
- Garantizar la seguridad y resiliencia de los activos estratégicos.
- Mejorar la investigación y persecución del cibercrimen.
- Impulsar la seguridad tanto en las empresas como en la ciudadanía.
- Potenciar la industria española de ciberseguridad, así como la generación y retención de talento.
- Contribuir a la seguridad internacional del ciberespacio.
- Desarrollar una cultura de ciberseguridad.

Capítulo 5. Se detalla la estructura de la ciberseguridad en el Sistema de Seguridad Nacional, constituida por el Consejo de Seguridad Nacional, Comité de Situación, Consejo Nacional de Ciberseguridad, Comisión Permanente de Ciberseguridad, Foro Nacional de Ciberseguridad y las Autoridades públicas competentes, así como los CSIRT[ix] de referencia nacionales en colaboración con los CSIRT autonómicos y privados.

El 26 de mayo de 2025, se publica en el Boletín Oficial del Estado la **Orden PJC/522/2025**[16], que oficializa el acuerdo del Consejo de Seguridad Nacional del 24 de abril de 2025 para iniciar la elaboración de una nueva Estrategia Nacional de Ciberseguridad.

La nueva **Estrategia nacional de ciberseguridad** busca:

- Actualizar las políticas nacionales para enfrentar las amenazas cibernéticas emergentes.
- Alinear la estrategia con las directrices de la Unión Europea y la Estrategia Europea de Ciberseguridad 2020 y la Directiva (UE) 2022/2555[17].
- Establecer medidas concretas para proteger infraestructuras críticas y servicios esenciales.
- Incorporar avances tecnológicos y fortalecer la resiliencia del ciberespacio nacional.

Este proceso refleja el compromiso de España por reforzar su ciberseguridad nacional y adaptarse a un entorno digital en constante evolución.

04

Ámbitos normativos y regulatorios

Normativa específica de ciberseguridad

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022

Modifica el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972, y deroga la Directiva (UE) 2016/1148. Su objetivo es reforzar la ciberseguridad de los Estados miembros mediante un marco más amplio y estricto, con sanciones reforzadas.

La Directiva NIS1 ya cubría la mayoría de los sectores del anexo I, como energía, transportes, salud, agua potable, infraestructuras de los mercados financieros, banca, infraestructura digital.

La NIS2 amplía este alcance e incorpora sectores adicionales, como el espacio, las aguas residuales, la administración pública y los servicios de gestión TIC.

En función del tipo de organización, su tamaño y sus ingresos, las entidades del anexo I se clasifican en dos categorías:

- **Esenciales:**
  - Grandes organizaciones con más de 250 personas empleadas o más de 50 millones de euros de ingresos anuales.
  - Administraciones públicas de los gobiernos centrales.
  - Operadores de servicios esenciales.
  - Otras organizaciones designadas por un Estado miembro.
- **Importantes:**
  - Organizaciones con más de 50 personas trabajadoras o más de 10 millones de euros de ingresos anuales.
  - Otras designadas por un Estado miembro.

A ambas categorías se les aplican los mismos requisitos de seguridad. No obstante, las entidades **esenciales** están sujetas a supervisión proactiva, mientras que las **importantes** solo lo están tras la notificación de un incidente. Las autoridades pueden imponer sanciones más elevadas a las primeras, incluidas multas y la suspensión temporal de cargos directivos.

El **anexo II** añade más sectores, todos ellos dentro de la categoría *importante*: servicios postales y de mensajería, alimentación, productos químicos, fabricantes, proveedores y proveedoras digitales, gestión de residuos, investigación, servicios de registro de nombres de dominio.

La directiva faculta a los Estados miembros a establecer listas nacionales de organizaciones esenciales e importantes, incluso si no cumplen los umbrales de ingresos o tamaño, cuando su impacto económico sea crítico o si se trata del único proveedor o proveedora de determinados servicios.

Los incidentes se comunican de forma escalonada: aviso inicial, seguimiento e informe final

En materia de **gestión de incidentes**, la NIS2 exige a las entidades notificar los incidentes significativos a las autoridades competentes o a los CSIRT de referencia en tres fases:

- En un plazo de 24 horas (informe inicial).
- En un plazo de 72 horas (informe detallado).
- Y en un mes (informe final).

Además, las entidades deben contar con un plan de gestión de incidentes, políticas de seguridad adecuadas y análisis de riesgos periódicos.

Las sanciones se endurecen con respecto a la NIS1:

- **Entidades esenciales:** hasta 10 millones de euros o un 2% de la facturación global.
- **Entidades importantes:** hasta 7 millones de euros o 1,4% de la facturación global.

La directiva también subraya la importancia de la formación en ciberseguridad para todo el personal, con el fin de reforzar la concienciación y la preparación frente a amenazas. Refuerza la cooperación entre Estados miembros y establece una red de intercambio de información más robusta.

Anteproyecto de ley de coordinación y gobernanza de la ciberseguridad

Elaborado por la Secretaría de Estado de Seguridad, tiene como finalidad reforzar la protección de redes y sistemas de información esenciales para la actividad económica y social. Afecta tanto a organizaciones con residencia fiscal en España como a aquellas establecidas en la UE que operen en territorio español.

El ámbito de aplicación incluye sectores críticos como energía, transporte, banca, sanidad, agua, infraestructuras digitales y administraciones públicas. Establece la obligación de notificar incidentes relevantes y de comunicar de inmediato a las personas usuarias de los servicios cualquier ciberamenaza significativa.

El anteproyecto crea la figura de la **persona responsable de la seguridad de la información**, que actuará como punto de contacto y coordinación técnica. En las organizaciones esenciales, esta persona deberá contar con acreditación oficial.

Asimismo, se contempla la creación del **Centro Nacional de Ciberseguridad**, adscrito a la Secretaría General de Presidencia del Gobierno, que funcionará como punto de contacto único con la Unión Europea y como autoridad en la gestión de crisis de ciberseguridad.

Centro Nacional de Ciberseguridad

Este organismo, además, se encargará de la dirección, impulso y coordinación en la materia, garantizará la cooperación intersectorial y transfronteriza con otras autoridades competentes.

Asimismo, la norma pone en pie una serie de autoridades de control encargadas de las **funciones de supervisión y ejecución**:

- El **Ministerio del Interior**, a través de la Oficina de Coordinación de Ciberseguridad de la Secretaría de Estado de Seguridad.
- El **Ministerio de Defensa**, a través del Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- El **Ministerio para la Transformación Digital y de la Función Pública**, a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y de Digitalización e Inteligencia Artificial.

El **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad** se encuentra **aprobado** por el Consejo de Ministros desde el 14 de enero de 2025 y superó su fase de notificación europea (TRIS) el 26 de mayo de 2025, pero a día de hoy no consta como ley aprobada en el BOE, lo que señala que su tramitación parlamentaria aún no ha finalizado.

Real Decreto 311/2022, de 3 de mayo de 2022

Regula el **Esquema Nacional de Seguridad**, con el objetivo de fortalecer la ciberseguridad y la resiliencia de los sistemas digitales esenciales.

Se aplica a la totalidad del sector público en los términos y condiciones en que se define a partir del artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

Del **artículo 5 al 11**, se exponen los principios básicos de seguridad:

- Seguridad como un proceso integral.
- Gestión basada en riesgos (identificar y mitigar amenazas cibernéticas).
- Prevención, detección, respuesta y conservación ante ciberataques.
- Existencia de líneas de defensa adecuadas frente a incidentes.
- Vigilancia continua y reevaluación periódica para identificar vulnerabilidades.
- Diferenciación de responsabilidades (responsable de la información, del servicio, de la seguridad y del sistema).

Del **artículo 12 al 30**, se establecen las medidas y requisitos mínimos de seguridad.

- Restricción de control de accesos y permisos en función de las necesidades operativas.
- Proteger la información almacenada y en tránsito.
- Monitorización y respuesta ante malware.
- Protocolos para una correcta gestión de incidentes y ciberataques.
- Continuidad del servicio a partir de planes de recuperación.

Del **artículo 31 al 34**, se establecen las auditorías y capacidad de respuesta ante incidentes.

- Auditorías periódicas de la seguridad.
- Creación de CSIRTs (equipos de respuesta rápida).
- Coordinación con el CCN-CERT[x] y otros organismos para articular la respuesta a los incidentes de seguridad.

Del **artículo 35 al 41**, se determinan la actualización y cumplimiento del ENS[xi].

- Alineación con regulaciones nacionales y europeas.
- Categorizar los sistemas de información.

Directiva (UE) 2016/1148, de 6 de julio de 2016

Establecida como norma por el Parlamento Europeo y del Consejo de 6 de julio de 2016, ha sido la primera norma europea en materia de ciberseguridad. Establece medidas para garantizar un nivel común de seguridad de las redes y de los sistemas de información en la UE.

Su ámbito de aplicación se centra en operadores y operadoras de servicios esenciales y en proveedores y proveedoras de servicios digitales. La norma exigía a los Estados miembros:

- Adoptar estrategias nacionales de ciberseguridad.
- Crear un Grupo de Cooperación para apoyar y facilitar la cooperación estratégica.
- Establecer una red de CSIRT (equipos de respuesta a incidentes de seguridad informática).
- Garantizar requisitos de seguridad y notificación de incidentes a las autoridades competentes.

Esta directiva fue derogada con la entrada en vigor de la **Directiva (UE) 2022/2555 (NIS2)**, que amplió sectores, reforzó las obligaciones y endureció las sanciones.

Marcos Nacionales de seguridad de las redes y sistemas de información

Regula la Estrategia Nacional de Seguridad de las Redes y Sistemas de Información, las autoridades nacionales competentes y punto de contacto único, y los equipos de respuesta a incidentes de seguridad informática y la cooperación a escala nacional.

Cooperación

En este capítulo, se desarrolla el grupo de cooperación, la Red de CSIRT y la cooperación internacional.

Además, se establece un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los estados miembros y desarrollar confianza y seguridad, y a fin de alcanzar un elevado nivel común de seguridad de las redes y sistemas de información en la UE.

El grupo ejerce sus funciones con arreglo a los programas de trabajo bienales a que se refiere el apartado 3.

Seguridad de las redes y sistemas de información de los operadores de servicios esenciales

Regula los **requisitos** en materia de seguridad y notificación de incidentes, y la aplicación y observancia.

Los Estados miembros velan por que los operadores de servicios esenciales tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan en sus operaciones. Habida cuenta de la situación, dichas medidas garantizarán un nivel de seguridad de las redes y sistemas de información adecuado en relación con el riesgo planteado.

Seguridad de las redes y sistemas de información de los proveedores de servicios digitales

En el presente capítulo se regulan los requisitos en materia de seguridad y notificación de incidentes, la aplicación y observancia, y la jurisdicción y territorialidad.

Los Estados miembros velan por que los proveedores de servicios digitales determinen y adopten medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información que se utilizan en el marco de la oferta de servicios en la Unión a que se refiere el Anexo III.

Habida cuenta de los avances técnicos, dichas medidas garantizarán un nivel de seguridad de las redes y los sistemas de información adecuado en relación con el riesgo planteado.

Normalización y notificación voluntaria

Se lleva a cabo la **regulación de la normalización y la notificación voluntaria**, por lo que los Estados miembros fomentan, sin imponer ni favorecer el uso de un tipo específico de tecnología, la utilización de normas y especificaciones aceptadas a nivel europeo o internacionalmente que sean pertinentes en materia de seguridad de las redes y sistemas de información.

Disposiciones finales

Se **dispone** de las sanciones, el procedimiento del Comité, la revisión, las medidas transitorias, la transposición, su entrada en vigor y los destinarios de la norma.

Los Estados miembros establecen el **régimen de sanciones** aplicables en caso de incumplimiento de las disposiciones nacionales aprobadas al amparo de la presente Directiva y adoptarán todas las medidas necesarias para garantizar su aplicación. Tales sanciones serán efectivas, proporcionadas y disuasorias.

En cuanto a la **transposición**, se prevé que los Estados miembros adoptarán y publicarán, a más tardar el 9 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Informarán de ello inmediatamente a la Comisión.

Además, incluye tres Anexos, el primero relativo a los Requisitos y funciones de los equipos de respuesta a incidentes de seguridad informática, el segundo relativo a los tipos de entidades a efectos del artículo 4, punto 4 y el tercero a los tipos de servicios digitales a efectos del artículo 4, punto 5.

Real Decreto 43/2021, de 26 de enero de 2021

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, que tiene como propósito reforzar la seguridad de sistemas de información y redes en España, con especial énfasis en los sectores que llevan a cabo la prestación de servicios esenciales o se encuentran integrados en el ámbito digital.

La presente normativa define las **medidas y obligaciones** que se deben adoptar tanto en los proveedores de servicios digitales, como aquellos de servicios esenciales. Se debe seguir la línea marcada por los estándares internacionales y las directrices europeas en la ciberseguridad.

Asimismo, la normativa implementa un **marco de actuación** que incluye la identificación y gestión en el entorno de análisis de riesgos, y las medidas técnicas y organizativas al objeto de la prevención, detección y respuesta frente a los incidentes de seguridad.

Los **principales aspectos** por los que se caracteriza se definen en:

- Adopción de **políticas de seguridad** en función del grado de criticidad de los diferentes servicios prestados.
- La realización de **análisis de riesgos**.
- **El carácter necesario de disponer de procesos de notificación y gestión de incidentes.**

A ello hay que añadir los mecanismos sobre la **supervisión y control** de la autoridad competente, así como las posibles infracciones y sanciones en caso de que se lleguen a incumplir las obligaciones previamente establecidas.

En definitiva, el Real Decreto 43/2021 consolida el **ecosistema de ciberseguridad a nivel nacional**, y asegura así que las infraestructuras críticas y los servicios digitales fortalezcan su protección frente a todo tipo de amenazas. Su debida implementación se considera clave a la hora de garantizar la continuidad y fiabilidad de los servicios esenciales, y continúa la línea progresista de modernización y protección de la Administración Electrónica[xii].


SCANNING...

Protección de Datos

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016

El **Reglamento 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[xiii] y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE tiene como objetivo la unificación de las normas y estándares sobre protección de datos en toda la Unión Europea, garantizar los derechos fundamentales relativos a la privacidad de la ciudadanía, implementar obligaciones para los responsables y encargados de tratamiento, y fomentar un entorno digital con plena seguridad.

En cuanto al **ámbito de aplicación**, , el Reglamento posee una aplicabilidad sobre la totalidad de entidades, tanto públicas como privadas, que traten datos personales de quienes residan en la UE, independientemente de donde se ubique la entidad en cuestión, por lo que, se incluye a entidades fuera de la UE, siempre y cuando sus actividades se encuentren orientadas al mercado europeo.

El Reglamento tiene su base en un elenco de **principios** que se consideran fundamentales a la hora de llevar a cabo cualquier tratamiento de datos:

1. **Licitud, lealtad y transparencia:** : Los datos personales deben tratarse de manera legítima, con una base jurídica adecuada, y los titulares de los datos deben ser informados de manera clara y sencilla sobre cómo se van a utilizar sus datos.
2. **Limitación de la finalidad:** Los datos que son recabados deben ser tratados para fines específicos, explícitos y legítimos, y no pueden ser utilizados para otra finalidad con la que fueron recogidos.
3. **Minimización de datos:** Ha de garantizarse que solo se recojan los datos que son estrictamente necesarios para la finalidad declarada, y evitar de esta forma una acumulación excesiva de la información.
4. **Exactitud:** Los datos deben ser exactos, y en su caso, actualizados. Por ello, se han de implementar mecanismos que faciliten su corrección o supresión en relación con la información inexacta.
5. **Limitación del plazo de conservación:** La conservación relativa a los datos personales no debe exceder el tiempo que se considere necesario para el cumplimiento de la finalidad con la que inicialmente se recabaron.
6. **Integridad y confidencialidad:** Se deben implementar medidas técnicas y organizativas que eviten el acceso no autorizado, pérdida o alteración de la información, o divulgación.
7. **Responsabilidad Proactiva:** Los responsables del tratamiento tienen la obligación de demostrar el cumplimiento de la totalidad de los principios por medio de políticas, documentación y auditorías de carácter interno.

En lo que respecta a los **derechos de los interesados**, el Reglamento General de Protección de Datos dispone a la ciudadanía un elenco de derechos que les permiten tener un poder de disposición y control sobre sus datos. Esta serie de derechos son: acceso, rectificación, supresión, limitación, portabilidad, oposición y derecho a no ser objeto de decisiones automatizadas.

Las **obligaciones** de responsables y encargados del tratamiento se determinan en:

1. **Implantación de medidas de seguridad:** Se deben adoptar las medidas técnicas y organizativas con el fin de garantizar la protección de los datos contra riesgos de ciberataque o de accesos indebidos.
2. **Evaluación de Impacto de la Protección de Datos:** En caso de que un determinado tratamiento pueda suponer un riesgo elevado para los derecho y libertades de las personas interesadas, se considera de carácter obligatorio la realización de una evaluación de impacto que resulte en la identificación de los riesgos e implique la aplicación de medidas para mitigar los mismos.
3. **Designación de Delegado de Protección de Datos:** En entidades de más de 250 personas trabajadoras o que traten datos sensibles a gran escala, se debe de nombrar un Delegado de Protección de Datos, que será la figura responsable de la supervisión del cumplimiento de la normativa y punto de contacto entre el responsable del tratamiento y la autoridad de control.
4. **Notificación de brechas de seguridad de la información:** Ante cualquier situación en la que se produzca una violación de la seguridad de los datos, las entidades han de notificar en un plazo máximo de 72 horas desde que se conoce, a la autoridad de control competente y, cuando puedan entrañar un alto riesgo, se deberá informar también a los interesados.
5. **Registro y documentación:** Se considera de carácter obligatorio el mantenimiento de un registro de actividades de tratamiento y la documentación que demuestre el cumplimiento de cada una de las obligaciones establecidas en el presente reglamento.

En lo que respecta a la realización de **transferencias internacionales** a terceros países, deben disponer de las garantías adecuadas acordes a un nivel de protección mínimo por medio de la aplicación de las cláusulas contractuales tipo o las reglas corporativas vinculantes.

En paralelo, la Comisión Europea cuenta con la capacidad de reconocer a un país, que no pertenece a la UE, como adecuado en cuanto al **nivel de protección**, lo que permite la realización de transferencias internacionales de datos sin la necesidad de medidas adicionales, a causa de una decisión de adecuación.

Cada uno de los Estados dispone de una o varias **autoridades de control independientes** que se encargan de supervisar y aplicar el efectivo cumplimiento del Reglamento General de Protección de Datos, es por ello que, dichas entidades poseen las potestades de investigar e implantar medidas de naturaleza correctiva y sanciones derivada de incumplimientos desde multas hasta el 4% del volumen global de negocios anuales, todo ello depende tanto de la gravedad como de la duración de la determinada infracción.

A ello hay que sumar el **mecanismo de cooperación y coordinación transfronteriza**, en donde en Reglamento General de Protección de Datos establece procesos de cooperación entre las distintas autoridades de control de los distintos Estados miembros de la Unión Europea, para así poder asegurar una aplicación informe en cuanto a la normativa y la gestión de incidentes de carácter transfronterizo.

Reglamento General de Protección de Datos ▶ Ley Orgánica de Protección de Datos y garantía de Derechos Digitales

Ley Orgánica 3/2018, de 5 de diciembre de 2018

La **Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales tiene como objetivo la regulación del tratamiento de datos personales y la protección de los derechos digitales de las personas.

Su **ámbito de aplicación** se determina en entidades públicas y privadas, para así poder garantizar que la totalidad de las organizaciones que tratan datos personales siguen el debido cumplimiento relativo a los estándares de privacidad y seguridad, de acuerdo con los principios contenidos en el Reglamento General de Protección de Datos[18].

En relación con los **principios y derechos fundamentales**, establece que los datos deben de ser tratados de manera lícita, leal y transparente, con limitación en relación con la finalidad, minimización, exactitud, limitación en el tiempo de conservación y seguridad. La ley adapta el marco jurídico para garantizar no exclusivamente la privacidad, sino también para que el empleo de las nuevas tecnologías no invada los derechos fundamentales de las personas interesadas.

Asimismo, se incluyen **derechos** concretos adaptados al ámbito digital, como el derecho de desconexión, el derecho al olvido y garantías restantes con el fin de proteger la intimidad en el entorno digital.

En cuanto a la **obligación** de quienes gestionan los datos, es decir, responsables y encargados de tratamiento, la normativa impone que deben implementar medidas técnicas y organizativas para garantizar la confidencialidad, integridad y disponibilidad de la información. En este ámbito también se incluye la realización de evaluaciones de impacto en la protección de datos en caso de que exista un alto riesgo para los derechos y libertades de los titulares de los datos, y la adopción de procedimientos para la gestión de incidentes.

Esta normativa se dispone a partir del **mecanismo de coherencia** con el **Reglamento General de Protección de Datos**, y determina en el ámbito nacional los aspectos que requieran de una especial atención en el contexto digital. Esta armonización deriva en la interoperabilidad de las medidas de protección de datos y ciberseguridad en España y en los Estados miembro de la Unión Europea, y genera un contexto normativo sólido y coordinado.

Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022

El **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 establece y tiene como principales **objetivos**:

- Las condiciones para la reutilización, dentro de la Unión, de determinadas categorías de datos que obren en poder de organismos del sector público.
- Un marco de notificación y supervisión para la prestación de servicios de intermediación de datos.
- Un marco para la inscripción voluntaria en un registro de las entidades que recojan y traten datos cedidos con fines altruistas.
- Un marco para la creación de un Comité Europeo de Innovación en materia de Datos.

El Derecho de la Unión y nacional en materia de protección de datos personales se aplicará a todos los datos personales tratados en relación con el presente Reglamento. Asimismo, el Reglamento no obliga a los **organismos del sector público** a permitir la **reutilización** de datos ni los exime de sus obligaciones en materia de confidencialidad que les imponga el Derecho de la Unión o el nacional.

Los datos personales deben tratarse de forma lícita, leal y transparente

Por consiguiente, el Reglamento se organiza y estructura en cuatro aspectos fundamentales:

1. **Reutilización de los datos del sector público:** En donde se facilita la reutilización de aquellos tipos de datos públicos que previamente se encontraban restringidos, e incluye tanto los datos personales anonimizados o bajo seudónimo, como los datos confidenciales.
2. **Uso de los servicios de intermediación de datos:** El Reglamento crea la figura del intermediario de datos con la finalidad de ayudar a compartir datos entre las distintas entidades o personas de una manera segura y controlada.
3. **Altruismo de datos:** A partir del presente concepto, se comparten datos de personas y organizaciones de manera voluntaria para el bien común.
4. **La Junta Europea de Innovación en materia de Datos:** A partir de lo dispuesto en el Reglamento, se crea dicha Junta con el objetivo de supervisar la implementación de manera uniforme del Reglamento en la UE.

Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018

El **Reglamento (UE) 2018/1724** del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por las instituciones y organismos de la Unión y las normas relativas a la libre circulación de dichos datos entre ellos o entre ellos y destinatarios establecidos en la Unión.

Este reglamento se **aplica** al tratamiento de datos personales por parte de todas las instituciones y organismos de la Unión Europea, e incluye el tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

Entre los **aspectos más destacados** se encuentran:

- Alineación con el Reglamento General de Protección de Datos[19].
- Principios de protección de datos.
- Derechos de los interesados.
- Delegados de Protección de Datos.
- Supervisión, cumplimiento normativo y sanciones.

Infraestructuras críticas

Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022

El principal objetivo de la **Directiva (UE) 2022/2557**, de 14 de diciembre de 2022, , relativa a la resiliencia de las entidades críticas y por la que se deroga la directiva (UE) 2008/114/CE del Consejo (Directiva CER) es establecer obligaciones y normas con el fin de que las entidades críticas aumenten su resiliencia en el mercado interior, así como sus capacidades para prevenir, proteger, responder y recuperarse ante posibles incidentes. Esta Directiva se entiende sin perjuicio del Derecho de la Unión en materia de protección de datos personales.

Entre los puntos clave de la normativa destaca:

1. **Ampliación del alcance a once sectores esenciales:**
   - Energía (electricidad, sistemas urbanos de calefacción, crudo, gas e hidrógeno).
   - Transporte (aéreo, ferrocarril, marítimo y fluvial, por carretera y público).
   - Banca
   - Infraestructuras de los mercados financieros
   - Sanidad
   - Agua potable
   - Aguas residuales
   - Infraestructura digital
   - Administración pública
   - Epacio
   - Producción, transformación y distribución de alimentos

2. **Obligaciones de los Estados miembros**
   - De acuerdo con el **artículo 6**, los Estados miembros tienen como fecha límite el 17 de julio de 2026 para **identificar** las entidades críticas de los once sectores indicados.
   - Deberán realizar una **evaluación de riesgo** a más tardar, el 17 de enero de 2026, y posteriormente a esta fecha, siempre que sea necesario y como mínimo cada cuatro años.
   - Cada Estado miembro deberá designar una o varias **autoridades competentes** que serán responsables de asegurar una correcta aplicación de la presente Directiva, así como un punto de contacto único que servirá como enlace y unión entre los otros puntos de los Estados miembros.
   - Ayudarán a las entidades críticas a **aumentar su resiliencia** (al desarrollar métodos de orientación, realizar ejercicios para probar la resiliencia, ofrecer asesoramiento y formación…).

3. **Obligaciones de las entidades críticas**
   - Realizar **evaluaciones de riesgos** periódicas, al considerar tanto los riesgos naturales como los de origen humano que puedan ocasionar un incidente.
   - Adoptar medidas para **garantizar su resiliencia** (controles de acceso, políticas de seguridad, planes de continuidad de negocio…).
   - Deberán establecer procedimientos para **notificar** incidentes que **perturben** la prestación de servicios esenciales a las autoridades competentes. El plazo establecido para una notificación inicial es de 24 horas desde el momento que se tiene conocimiento del incidente y un mes como máximo, para un informe detallado. La información que especificar es el número y porcentaje de personas usuarias afectadas, la duración y la zona geográfica afectada.

Si el incidente afecta a **seis o más** Estados miembros, las autoridades competentes deberán notificarlo a la Comisión Europea.

4. **Grupo de Resiliencia de las Entidades Críticas**

Establecimiento del Grupo con el objetivo de apoyar la **implementación de la Directiva CER** en la Unión Europea. Entre sus funciones se encuentra facilitar la cooperación entre los Estados miembros, analizar estrategias para mejorar la resiliencia de las entidades críticas, promover el intercambio de información sobre amenazas y riesgos, supervisar la aplicación correcta de las medidas indicadas en la Directiva.

- **Transposición al ordenamiento jurídico interno**

El Proyecto de Ley de Protección y Resiliencia de las Entidades Críticas ha sido aprobado por el Consejo de Ministros el 17 de marzo de 2026, en segunda vuelta, a propuesta del Ministerio del Interior. Esto supone un avance relevante en su tramitación, ya que el Gobierno ha dado luz verde al texto normativo para su remisión a las Cortes Generales, donde deberá continuar el procedimiento legislativo ordinario.

A pesar de esta aprobación por parte del Consejo de Ministros, la ley aún no ha entrado en vigor, dado que no consta su aprobación parlamentaria definitiva ni su publicación en el Boletín Oficial del Estado.

La norma se encuentra ahora en fase de tramitación parlamentaria en el Congreso, tras lo cual deberá pasar por el Senado antes de su promulgación y publicación oficial. En consecuencia, el texto ya no es un anteproyecto, pero tampoco es todavía una ley vigente, situándose actualmente en la fase de proyecto de ley en tramitación parlamentaria.

A los sectores estratégicos les ampara una normativa especial

Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022

El **Reglamento (UE) 2022/2554** del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011 (Reglamento DORA), tiene como objetivo fortalecer la resiliencia operativa digital del sector financiero de la Unión Europea, y establece un marco normativo armonizado para la gestión del riesgo de las tecnologías de la información y la comunicación.

El presente reglamento se **aplica** a:

- Entidades de crédito, de pago, de dinero electrónico y de pensiones de jubilación.
- Proveedores de servicios de información sobre cuentas, criptoactivos, notificación de datos, financiación participativa y terceros de las tecnologías de la información y la comunicación.
- Empresas de inversión, fondos de inversión alternativos, sociedades gestoras, agencias de calificación crediticia y administradores de índices de referencia cruciales.
- Registros de operaciones y titulizaciones, depositarios centrales de valores, contrapartes centrales y centros de negociación.
- Seguros, intermediarios de seguros y reaseguros.

Como **puntos más importantes** se destacan:

- La **necesidad de resiliencia digital** en el sector financiero. El aumento de la digitalización ha amplificado la dependencia de las tecnologías de la información y la comunicación, lo que hace que el sistema financiero sea más vulnerable a ciberamenazas y fallos tecnológicos. Además, las interconexiones entre entidades y proveedores externos amplifican también el riesgo de incidentes de ciberseguridad.

- La necesidad de **armonización regulatoria**, es decir, deben desarrollarse normas comunes para la gestión de las tecnologías de la información y la comunicación en todas las entidades de la Unión Europea. Se busca eliminar disparidades legislativas y enfoques de regulación desiguales para evitar obstáculos al funcionamiento del mercado.

- Se exige que las entidades financieras implementen un marco sólido de **gestión del riesgo** de las tecnologías de la información y la comunicación, con políticas para prevención, detección, respuesta y recuperación ante incidentes cibernéticos. Además de requisitos específicos para la externalización de servicios de las tecnologías de la información y la comunicación, especialmente para los proveedores terceros críticos.

- La obligación de **notificación de incidentes**, es decir, las entidades financieras deben informar rápidamente sobre los incidentes graves relacionados con las tecnologías de la información y la comunicación a las autoridades nacionales competentes. Se busca una coordinación eficaz entre las autoridades de supervisión, la Agencia de la Unión Europea para la Ciberseguridad y otras instituciones.

- El establecimiento de requisitos para que las entidades financieras realicen **pruebas regulares** para sus sistemas de información. Se incluyen pruebas avanzadas de penetración para las entidades más críticas.

- La implementación de un **marco de supervisión** para los proveedores de servicios esenciales para el sector financiero. Se busca evitar riesgos sistemáticos derivados de la concentración de servicios en pocos proveedores.

- Se fomenta la **cooperación** entre entidades financieras para compartir inteligencia sobre ciberataques, al respetar la normativa de protección de datos.

- Se establecen **requisitos diferenciados** para grandes entidades financieras y microempresas, al reducir la carga administrativa para las más pequeñas.

Las normas de ciberseguridad de la UE están enfocadas a mejorar prevención, cooperación y respuesta ante incidentes

Ley 8/2011, de 28 de abril de 2011

La **Ley 8/2011**, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, 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 del Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas.

La presente Ley se **aplica** a las infraestructuras críticas ubicadas en el territorio nacional vinculadas a los sectores estratégicos definidos en el anexo de esta Ley.

La ley consta de **18 artículos** estructurados en tres títulos:

1. **Del artículo 1 al 4, se establecen las Disposiciones generales.**

   Se establece como objetivo de la Ley la **coordinación de la protección de infraestructuras críticas** a través de la colaboración entre administraciones públicas y operadores privados. Además, se definen términos relevantes como servicio esencial, infraestructuras estratégicas y críticas, análisis de riesgos u operador crítico. Por último, se introduce el Catálogo Nacional de Infraestructuras Estratégicas, gestionado por el Ministerio del Interior, que incluye infraestructuras clasificadas como críticas o críticas europeas.

2. **Del artículo 5 al 13, se dispone del Sistema de Protección de Infraestructuras Críticas.**

   Se regulan los **órganos e instrumentos de planificación** que se integran en el Sistema de Protección las Infraestructuras Críticas.

   Se crea el **CNPIC** (Centro Nacional para la Protección de las Infraestructuras Críticas), dependiente de la Secretaría de Estado de Seguridad.

   Además, se detalla quiénes son agentes del Sistema (lo que incluye ministerios, comunidades autónomas y operadores críticos) y se exponen las funciones de la Comisión Nacional para la Protección de Infraestructuras Críticas y el Grupo de Trabajo Interdepartamental.

3. **Del artículo 14 al 18, se exponen los instrumentos y comunicación del sistema.**

   Se establecen las **medidas de protección y procedimientos** que deben aplicarse. Entre ellos se introduce el Plan Nacional de Protección de Infraestructuras Críticas, los Planes Estratégicos Sectoriales, los de Seguridad del Operador y los de Protección Específicos.

   Los operadores críticos tienen la obligación de nombrar un Responsable de Seguridad y Enlace, además de un Delegado de Seguridad para cada infraestructura crítica.

   Asimismo, la ley consta de cuatro disposiciones adicionales y cinco finales en las que se establece que la ley se desarrolla bajo el marco constitucional de seguridad pública y se incorpora la Directiva (UE) 2008/114/CE[20].

Real Decreto-ley 7/2022 ▶ Real Decreto 443/2024

Real Decreto 704/2011, de 20 de mayo de 2011

Por él se aprueba el Reglamento de protección de Infraestructuras Críticas, con el objetivo de desarrollar el marco previsto en la Ley 8/2011[21], establece dos propósitos:

1. Catalogación de las **infraestructuras críticas**, es decir, las consideradas como esenciales. Se recogen en el Sistema Nacional de Protección de Infraestructuras Críticas, un compendio de las instituciones, órganos y empresas, tanto del sector público como del privado, con responsabilidad en el funcionamiento de los servicios esenciales o en la seguridad de las personas. Algunos ejemplos incluyen el CNPIC[xiv], ministerios, Comunidades Autónomas, Corporaciones locales, o Grupos de trabajo sectoriales, entre otros.

2. Determinación de las **medidas de protección** para estas infraestructuras, e incluye la seguridad en tecnologías de la información y comunicaciones.

El **ámbito de aplicación** del presente Reglamento será el previsto por el artículo 3 de la Ley 8/2011, de 28 de abril.

Un aspecto importante de la Ley 8/2011[22] es su definición de las **infraestructuras críticas**. "*Aquellas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales*".

Define, además, un conjunto de textos normativos con medidas de protección a ejecutar por los integrantes del del Sistema de Protección de Infraestructuras Críticas.

Estos documentos detallan las actuaciones que deben realizar los integrantes del sistema. Incluyen:

- **Planes Estratégicos Sectoriales (PES)**, asignados a cada sector considerado crítico.
- **Plan de Seguridad del Operador (PSO)** y **Plan de Protección Específico (PPE)**, que todo operador crítico debe presentar.

Entre las medidas de la normativa se encuentra también la organización de la **información completa** de las características de cada una de las infraestructuras estratégicas nacionales. Para ello, se han habilitado plataformas específicas que lo facilitan.

En definitiva, el marco previsto en la Ley 8/2011 establece toda una serie de medidas de profundo calado para los operadores críticos para garantizar su continuidad y protección.

Seguridad en productos digitales y telecomunicaciones

Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014

El **Reglamento eIDAS** regula la identificación electrónica y los servicios de confianza en las transacciones digitales dentro del mercado interior de la UE. Sustituye la Directiva 1999/93/CE, garantiza la seguridad y el reconocimiento mutuo de estos servicios en todos los Estados miembros y promueve la interoperabilidad entre sistemas.

Aplica a cualquier persona, entidad u organismo público que utilice medios electrónicos para identificarse, firmar documentos o intercambiar información de forma segura. Su entrada en vigor supuso un avance clave en la modernización del mercado digital europeo.

Se basa en los siguientes **principios** esenciales:

- **Reconocimiento transfronterizo:** Los sistemas de identificación electrónica de un país miembro deben ser aceptados en el resto de los Estados de la UE.
- **Seguridad jurídica y técnica:** Se establecen estándares claros para garantizar la fiabilidad de las firmas electrónicas, los sellos digitales y otros mecanismos de autenticación.
- **Interoperabilidad:** Busca que las soluciones digitales de distintos países sean compatibles entre sí, y facilitar su uso en entornos internacionales.

- **Confianza y protección:** Se exige que los proveedores de servicios cumplan con estrictos criterios de seguridad para proteger la integridad de los datos y las identidades digitales

El presente reglamento establece un marco normativo para proveedores de servicios de confianza, y exigir requisitos específicos como:

- **Medidas de seguridad avanzadas:** Se requiere la adopción de protocolos que eviten la alteración o falsificación de documentos electrónicos.

- **Supervisión y certificación:** Solo los proveedores debidamente acreditados pueden ofrecer servicios de confianza reconocidos por la UE.

- **Información clara y transparente:** Quien lo use debe conocer las condiciones y garantías de los servicios digitales que utilizan.

Estos servicios tienen una especial relevancia en el contexto de la ciberseguridad, ya que fortalecen la integridad y confidencialidad de las interacciones electrónicas, y reducir el riesgo de fraudes o suplantaciones de identidad.

Uno de los pilares de eIDAS es el desarrollo de sistemas de identificación digital que permitan a la ciudadanía acceder a servicios públicos y privados de manera remota y segura. Esta medida facilita la digitalización de la administración pública y refuerza la confianza en el comercio electrónico.

Uno de los aspectos clave del reglamento es el reconocimiento mutuo obligatorio de los esquemas de identificación electrónica entre los países de la UE. Esto permite operar en distintos Estados sin barreras burocráticas innecesarias.

La aplicación del reglamento refuerza la seguridad digital en ámbitos como la protección de las transacciones electrónicas. La firma electrónica y otros servicios de confianza ayudan a prevenir la manipulación o alteración de documentos digitales.

De otra parte, en cuanto a la prevención del fraude en identidad digital, se establecen mecanismos que impiden la suplantación de identidades en servicios electrónicos.

Por tanto, esta normativa representa un avance fundamental en la construcción de un entorno digital seguro y confiable dentro de la UE. Al regular la identificación electrónica y los servicios de confianza, facilita la interoperabilidad entre países y refuerza la protección de datos y transacciones digitales.

EIDAS impulsa la identificación digital y los servicios de confianza, clave para transacciones seguras y prevención del fraude en la UE

Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024

Por él se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (Reglamento eIDAS 2) tiene por objeto garantizar el correcto funcionamiento del mercado interior y la existencia de un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza utilizados en toda la UE.

Su la finalidad de permitir y facilitar que las personas físicas y jurídicas ejerzan el derecho a participar en la sociedad digital de una forma segura y a acceder a los servicios del sector público y privado en línea en toda la UE. Además:

- Define las condiciones para que los Estados miembros reconozcan los medios de identificación electrónica de personas y entidades de otros países de la UE, incluidas las carteras europeas de identidad digital.
- Regula los servicios de confianza, especialmente en las transacciones electrónicas.
- Proporciona el marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo, los documentos digitales, los servicios de entrega certificada, la autenticación de sitios web, el archivo electrónico, la declaración electrónica de atributos, los dispositivos de creación de firmas y sellos, y los libros mayores electrónicos.

Amplía el ámbito de aplicación del marco de identidad digital en la UE. Promueve una infraestructura digital armonizada que facilita la identificación electrónica transfronteriza y refuerza la confianza en los servicios digitales.

Para ello, introduce un sistema común de identidad digital que reduce los obstáculos entre Estados y permite que cualquier persona residente en la UE acceda a los beneficios de la digitalización. Al mismo tiempo, mejora la transparencia y protege los derechos digitales.

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019

Esta normativa involucra a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y tiene que ver con la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 (Reglamento sobre la Ciberseguridad).

Establece, por una parte, los **objetivos**, tareas y aspectos organizativos a ENISA y, por otro, un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la UE.

En cuanto al **ámbito de aplicación**, se entenderá sin perjuicio de las competencias de los Estados miembros en materia de actividades relacionadas con la seguridad pública, la defensa, la seguridad nacional y las actividades del Estado en ámbitos del Derecho penal.

En aspectos generales, delinea la **estructura** y las **responsabilidades** clave de **ENISA**. Además, establece un marco de certificación de ciberseguridad para productos, servicios y procesos de TIC en toda la UE. Este reglamento es un componente fundamental de la estrategia de la UE para mejorar la ciberseguridad y crear un mercado único digital armonizado.

Establece de forma permanente la ENISA, y refuerza su papel de apoyo a los estados y a las instituciones de la UE para mejorar la ciberseguridad, servir de centro de conocimientos especializados y reducir la fragmentación del mercado.

Una parte importante del reglamento eIDAS se dedica a crear un marco europeo de certificación en ciberseguridad. Este define esquemas comunes para toda la UE, con el objetivo de aumentar la confianza en productos, servicios y procesos relacionados con las TIC.

Los esquemas indican niveles de garantía de seguridad y sustituyen los marcos nacionales por un enfoque coherente a escala europea.

La **ENISA** opera bajo un consejo de administración, un consejo ejecutivo y un grupo consultivo, que garantizan su funcionamiento eficaz y alineado con sus responsabilidades ampliadas. Además, se crea el **Grupo Europeo de Certificación de la Ciberseguridad**, encargado de apoyar el desarrollo y la aplicación del marco común.

El reglamento también incluye disposiciones para evaluar periódicamente el impacto de ENISA y la eficacia de los sistemas de certificación. La primera revisión exhaustiva se programó para 2024, y las siguientes se realizarán cada cinco años.

El Reglamento sobre la Ciberseguridad crea un marco europeo común para certificar productos, servicios y procesos TIC

Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018

Por ella se establece el **Código Europeo de las Comunicaciones Electrónicas** (CECE), adoptada con el fin de modernizar y unificar la regulación de las telecomunicaciones dentro de la UE. Esta normativa reemplaza varias directivas previas y establece un marco normativo común que fomenta la competencia, seguridad y accesibilidad en las redes y servicios de comunicaciones electrónicas.

El CECE se adapta a los cambios tecnológicos y a la transformación digital, al abordar **nuevas formas de comunicación**, como los servicios en línea de mensajería y llamadas por Internet, además de consolidar las normas aplicables a los operadores tradicionales.

Su enfoque en la **seguridad, interoperabilidad y modernización de las redes digitales** fortalece la estrategia de ciberseguridad europea y sienta las bases para un mercado más competitivo y seguro.

Desde la perspectiva española, la implementación de esta directiva refuerza la seguridad en las infraestructuras de telecomunicaciones y mejora la protección de las personas usuarias en el entorno digital. Dentro de un análisis comparativo de las normativas de ciberseguridad en España y la UE, el CECE es una pieza fundamental para garantizar la **resiliencia y protección de las comunicaciones electrónicas en toda Europa.**

Esta directiva se **aplica** a:

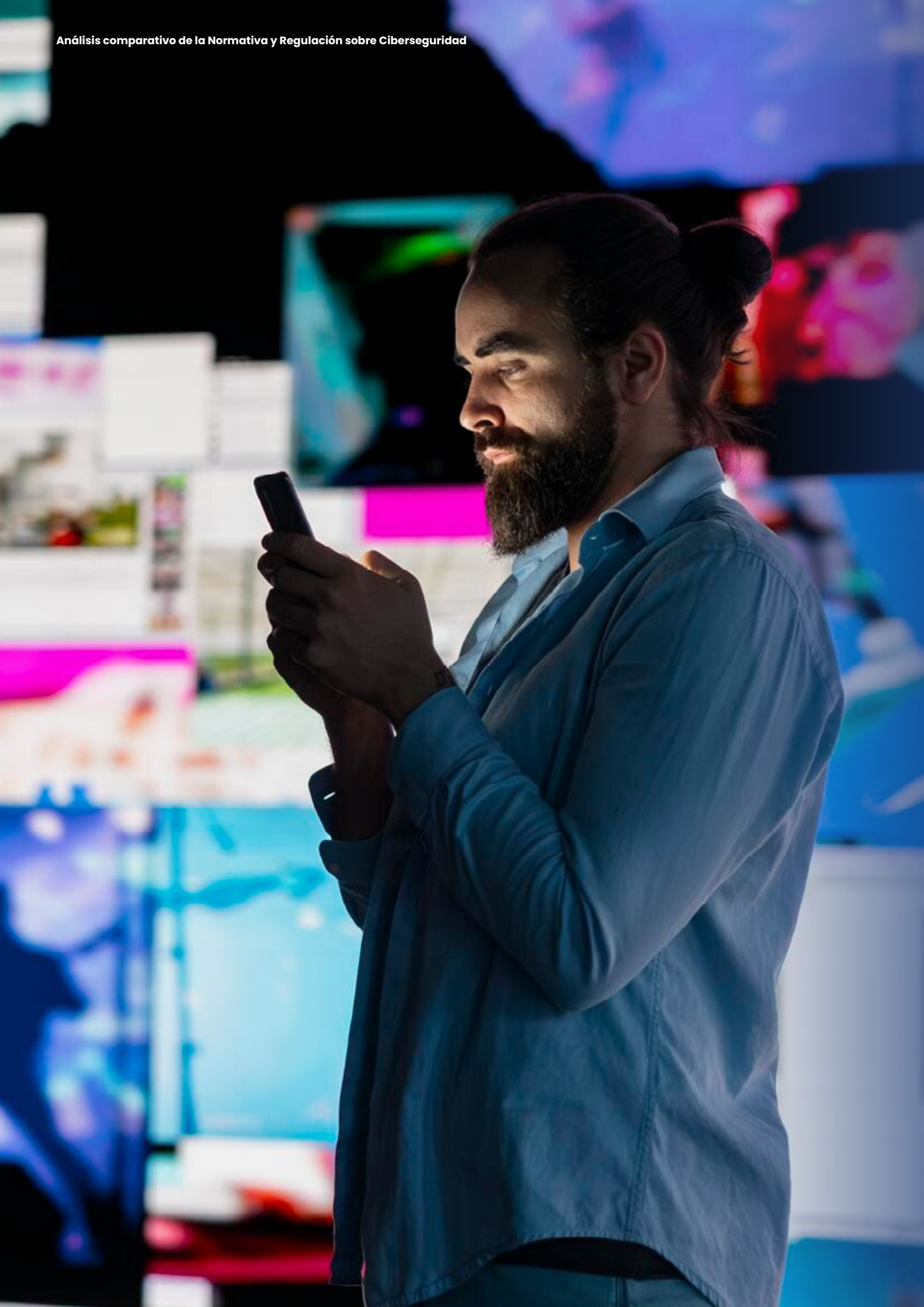
- **Operadores y proveedores de servicios de telecomunicaciones**, e incluye aquellos que gestionan infraestructuras físicas y redes de comunicación.
- **Plataformas digitales y aplicaciones de mensajería instantánea**, como WhatsApp, Skype o Telegram, que ahora están sujetas a regulaciones similares a las de las empresas tradicionales de telecomunicaciones.
- **Aspectos de seguridad digital y ciberprotección**, al establecer medidas obligatorias para la protección de redes y la gestión de incidentes de seguridad.
- **Fomento de la conectividad y despliegue de redes avanzadas**, lo que incluye la expansión de infraestructuras 5G y fibra óptica en toda la UE.

Uno de los ejes centrales del CECE es la resiliencia de las redes de telecomunicaciones ante amenazas cibernéticas. Para ello, impone obligaciones a los operadores de telecomunicaciones y plataformas digitales.

El CECE introduce normas armonizadas para la **gestión del espectro radioeléctrico**, elemento clave en el despliegue de redes 5G. Entre las disposiciones más relevantes se encuentran la asignación eficiente del espectro de toda la UE, los incentivos a la inversión en redes de alta capacidad y la evaluación de los riesgos relativos a la implementación de 5G.

El CECE refuerza la **protección de los derechos de las persona**s en el uso de redes de comunicación electrónica. Algunas medidas clave incluyen:

- **Transparencia en los contratos con operadores**, al asegurar que las personas usuarias reciban información clara sobre costos, calidad del servicio y velocidad de conexión.
- **Facilitación del cambio de operador**, y mejorar los procesos de **portabilidad numérica** al reducir las restricciones en los contratos.
- **Garantía del acceso universal a Internet,** al obligar a los Estados miembros a garantizar una conectividad mínima para todos y todas.



Directiva (UE) 2014/53 del Parlamento Europeo y del Consejo, de 16 de abril de 2014

Relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE (Directiva RED). Establece un marco regulador para para la comercialización y la puesta en servicio en la Unión Europea de equipos radioeléctricos.

Su **objetivo** es garantizar que los equipos cumplan unos requisitos esenciales de seguridad, compatibilidad electromagnética y uso eficiente del espectro radioeléctrico. Esta directiva reemplaza a la anterior Directiva 1999/05/CE[23] y fue transpuesta en España mediante el Real Decreto 188/2016[24] .

La **directiva RED** regula los equipos radioeléctricos en el mercado interior de la UE. Estos equipos no están sujetos a la directiva 2014/35/UE, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos eléctricos diseñados para funcionar dentro de unos límites de tensión, salvo en lo previsto en el artículo 3.1.a) de la propia directiva RED.

Quedan fuera de su ámbito de aplicación, según el anexo I, dispositivos como los equipos de radioaficionados, productos diseñados exclusivamente para investigación y desarrollo, ciertos equipos marinos regulados por normativa específica y aquellos destinados a seguridad pública, defensa o fuerzas del orden, que se rigen por marcos distintos.

La directiva distingue entre los agentes económicos que participan en la cadena de suministro: fabricantes, representantes autorizados, importadores y distribuidores.

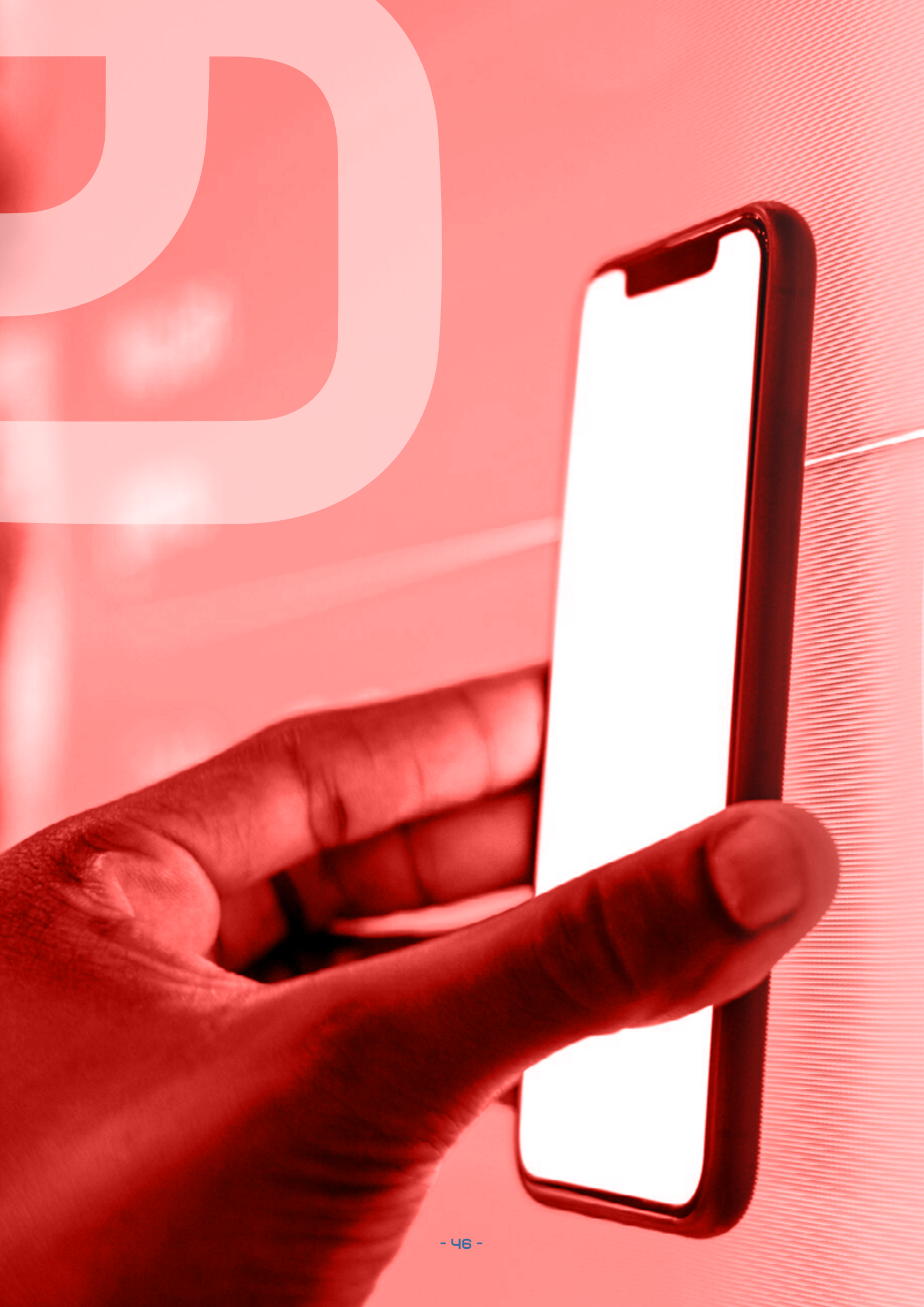
- El fabricante debe garantizar que el producto cumple los requisitos esenciales, realizar la evaluación de conformidad, emitir la declaración UE de conformidad y colocar el marcado CE.
- El importador, al introducir productos desde fuera del espacio económico europeo, tiene que comprobar que el fabricante ha seguido todos los procedimientos exigidos antes de su comercialización.
- El distribuidor debe verificar que los productos llevan el marcado CE, incluyen la documentación técnica y la declaración UE de conformidad, y que durante el almacenamiento y transporte se mantienen las condiciones necesarias para preservar su conformidad.

Uno de los elementos clave de la directiva es la definición de los requisitos esenciales que deben cumplir los equipos: protección de la salud y la seguridad de personas, animales domésticos y bienes materiales; compatibilidad electromagnética; y uso eficiente del espectro radioeléctrico, para evitar interferencias perjudiciales. Para demostrar la conformidad, se establecen varios procedimientos de evaluación.

También se regulan las restricciones de uso. Si existen limitaciones en determinados Estados miembros o zonas geográficas, deben indicarse de forma clara en el embalaje y en las instrucciones del producto.

La directiva garantiza la libre circulación de los equipos radioeléctricos en el mercado interior de la UE, siempre que cumplan sus requisitos. Se permite mostrar equipos no conformes en ferias o exposiciones, siempre que se indique de forma explícita que no están disponibles para la venta o el uso hasta que se ajusten a la normativa.

Este marco legal sirve de base para otras normativas sobre ciberseguridad y refleja una evolución hacia una regulación más estricta y transversal en materia de seguridad digital.



Real Decreto 4/2010, de 8 de enero de 2010

El **Real Decreto 4/2010**, de 8 de enero, por el que se regula el **Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica**, se centra en determinar las directrices, procedimientos y estándares que deben seguir las administraciones públicas para garantizar el intercambio y la integración eficaz de información en los sistemas.

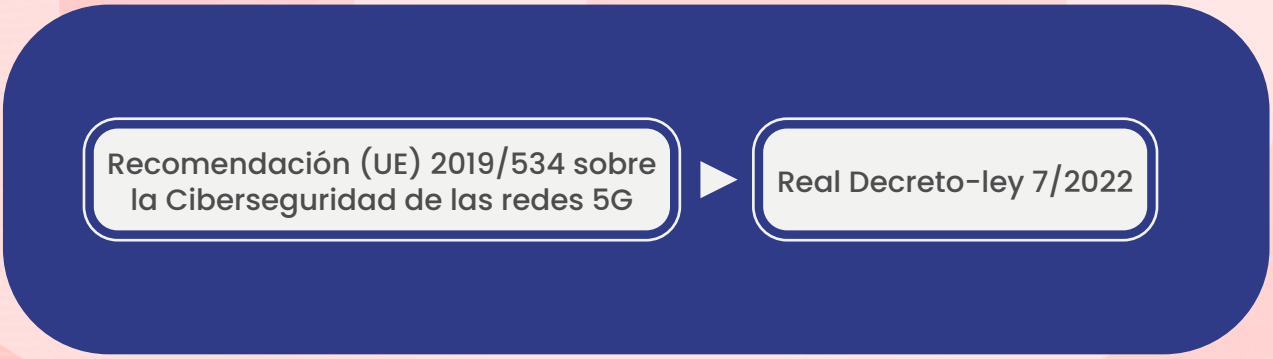
La presente ley, en los términos expresados en su disposición final primera, será de aplicación:

- A las administraciones públicas; o sea, Administración General del Estado, administraciones de las comunidades autónomas y entidades que integran la administración local, así como las entidades de derecho público vinculadas o dependientes de las mismas.
- A la ciudadanía en sus relaciones con las administraciones públicas.
- A las relaciones entre las distintas administraciones públicas.

Este marco normativo impulsa la adopción de soluciones basadas en estándares abiertos y procesos técnicos, por lo que facilita la interoperabilidad tanto en el plano técnico como semántico en los distintos organismos a nivel estatal y local.

En cuanto al ámbito de la ciberseguridad, el real decreto destaca la importancia de implementar las medidas que garanticen la **confidencialidad, disponibilidad, integridad y autenticidad** de la información objeto de intercambio. Por consiguiente, el diseño y gestión de los sistemas deben minimizar los riesgos y vulnerabilidades, y garantizar el intercambio de datos y documentos electrónicos de una forma segura.

La normativa es un pilar fundamental para la transformación digital de la Administración. Establece un marco común de interoperabilidad que sienta las bases de la integración tecnológica. Además, refuerza los estándares de ciberseguridad necesarios para el buen funcionamiento de los servicios públicos electrónicos.



Real Decreto-ley 7/2022, de 29 de marzo de 2022

Establece los requisitos para garantizar la **seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación (5G)** en España.

Este real decreto-ley se aplica a:

- Operadores 5G
- Suministradores 5G
- Las personas usuarias corporativas 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación

Se establecen, asimismo, **medidas** para proteger las redes 5G contra amenazas y vulnerabilidades, para la protección de datos personales y privacidad de las personas usuarias. Se establece la evaluación periódica de riesgos y la implementación de las medidas de mitigación adecuadas.

Respecto a **ciberseguridad**, se mencionan **aspectos clave** como la necesidad de que operadores y proveedores de servicios 5G realicen análisis periódicos de riesgos, además de implementar medidas para mitigar las amenazas encontradas. Se establece la obligación de garantizar la confidencialidad de la información y se implantan procedimientos específicos para la gestión de incidentes.

Real Decreto-ley 7/2022 ▶ Real Decreto 443/2024

Real Decreto 443/2024, de 30 de abril de 2024

Por este Real Decreto se aprueba el **Esquema Nacional de Seguridad** en redes y servicios 5G. Su objetivo es establecer un marco normativo específico para proteger estas redes y servicios en frente a amenazas y vulnerabilidades. Reconoce la importancia de estas infraestructuras tanto para la seguridad nacional como para la economía, y fija los requisitos mínimos y las medidas de seguridad que deben cumplir las administraciones públicas, los operadores de red y los proveedores de servicios.

El ámbito de aplicación se extiende a todas las entidades que gestionan servicios relacionados con el 5G, incluidas las administraciones públicas, los operadores de telecomunicaciones y los proveedores de servicios digitales que utilizan o dependen de estas infraestructuras.

Los **principios y requisitos mínimos** de seguridad sobre los que se sustenta el Real Decreto se formalizan en los siguientes:

1. **Evaluación y gestión de riesgos**: Es necesario realizar análisis periódicos del entorno 5G para identificar, evaluar y mitigar amenazas potenciales de forma proactiva.

2. **Medidas técnicas y organizativas**: En el ámbito técnico, se contemplan protocolos de cifrado, segmentación de red, autenticación robusta, control de accesos y detección de intrusiones. En el organizativo, se incluyen planes de contingencia, protocolos de respuesta ante incidentes, formación continua del personal y auditorías internas de seguridad.

3. **Cadena de suministro y equipos críticos**: Los equipos y componentes empleados deben cumplir con estándares de seguridad certificados, con el fin de minimizar al máximo el riesgo de injerencias externas.

Los **mecanismos de supervisión y control** que establece el real decreto deben permitir un monitoreo continuo sobre el estado de seguridad relativo a las infraestructuras 5G por medio de los sistemas de alerta temprana y los centros de operaciones de ciberseguridad. Por consiguiente, la realización de auditorías de carácter periódico debe verificar el cumplimiento del elenco de requisitos y, en los casos que proceda, para la obtención de certificaciones que respalden la solidez del sistema de seguridad que se haya implantado.

El Esquema Nacional de Seguridad 5G fija requisitos mínimos para proteger redes, servicios y cadenas de suministro

Ciberresiliencia

Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024

Versa sobre requisitos horizontales de ciberseguridad para productos con elementos digitales, tiene como objetivo establecer requisitos horizontales sobre ciberseguridad para productos con elementos digitales comercializados en la Unión Europea (Ley de Ciberresiliencia).

La normativa busca garantizar la seguridad de estos productos y proteger al ciudadano de aquellos productos que no cumplan con requisitos de ciberseguridad.

Es **aplicable** a los productos con elementos digitales comercializados cuya finalidad prevista o uso razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red.

De conformidad con el presente Reglamento, la definición de "productos con elementos digitales" se entiende por: "Producto consistente en programas o equipos informáticos y sus soluciones de procesamiento de datos remoto, incluidos los componentes consistentes en programas informáticos o equipos informáticos que se introduzcan en el mercado por separado".

La **Ley de Ciberresiliencia o CRA** clasifica los productos en función de su riesgo: productos importantes (Anexo III) y productos críticos (Anexo IV).

1. Productos importantes:

- Clase I. Productos de riesgo moderado que solo requieren autoevaluación del fabricante (sistemas operativos, gestores de contraseñas, sistemas de gestión de redes…).
- Clase II. Productos de riesgo alto que requieren de certificación de terceros (cortafuegos[xv], microprocesadores resistentes a manipulaciones, sistemas de detección y prevención de intrusiones…).

2. Productos críticos: Mayor impacto en la seguridad, por lo que requieren controles más estrictos en su comercialización (dispositivos de equipos informáticos con cajas de seguridad, tarjetas inteligentes…).

Objetivos principales de la normativa:

1. Seguridad en todo el ciclo de vida del producto. Los fabricantes deben garantizar la ciberseguridad desde la planificación hasta el mantenimiento. Están obligados a realizar una evaluación documentada de riesgos y a cumplir los requisitos del **Anexo I**, que recogen tanto las propiedades de los productos con elementos digitales como la gestión de vulnerabilidades. Solo podrán comercializarse los productos que cumplan estos requisitos.

2. Información transparente para las personas usuarias. Se debe ofrecer documentación clara sobre el uso seguro de los productos y las actualizaciones de seguridad disponibles. El **Anexo II** detalla la información mínima que debe acompañar a cada producto.

3. Gestión y notificación de vulnerabilidades. Los fabricantes deberán mitigar vulnerabilidades e informar al CSIRT coordinador y a la Agencia de Ciberseguridad de la Unión Europea a través de la plataforma establecida en el artículo 16. Los plazos de notificación son:

- Alerta temprana: En un máximo de 24 horas desde que se detecta el incidente.
- Informe inicial de vulnerabilidad: En 72 horas.
- Informe final: En 14 días, con la información prevista en el artículo 14.

4. Requisitos de comercialización. El marcado **CE** es obligatorio para todos los productos con elementos digitales. Este sello certifica que el fabricante ha realizado las evaluaciones necesarias para cumplir la normativa de la Unión Europea, garantizando su seguridad y permitiendo su libre circulación.

5. Marco normativo integrado. La normativa se alinea con otros marcos como Reglamento General de Protección de Datos[25], para facilitar el cumplimiento por parte de los fabricantes.

Régimen sancionador

- Incumplimiento de requisitos de seguridad: multas de hasta 15 millones de euros o el 2,5% de la facturación global.
- Incumplimiento en la notificación de incidentes o vulnerabilidades: multas de hasta 10 millones de euros o el 2% de la facturación global.

Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024

Por él se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la UE para detectar ciberamenazas e incidentes, prepararse y responder a ellos, y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad) establece aquellas **medidas** para reforzar las capacidades de la UE para **detectar amenazas e incidentes** de ciberseguridad, **prepararse** para ellos y responder ante los mismos, en concreto por medio de la creación de:

- Una **red paneuropea de centros cibernéticos** a fin de desarrollar y mejorar las capacidades coordinadas de detección y la conciencia situacional común.
- Un **mecanismo de emergencia** en ciberseguridad para ayudar a los Estados a prepararse para incidentes de ciberseguridad significativos, a gran escala y equivalentes a gran escala, y a responder a ellos, atenuar sus repercusiones y e iniciar la recuperación de ellos, así como ayudar a otras personas usuarias a responder a incidentes de ciberseguridad significativos y equivalentes a gran escala.
- Un **mecanismo europeo de revisión de incidentes** de ciberseguridad para revisar y evaluar incidentes de ciberseguridad significativos o a gran escala.

Este reglamento se aplica en todos los Estados miembros para reforzar la posición competitiva de la industria y los servicios en la economía digital, incluidas las microempresas, las pequeñas y medianas empresas, y las empresas emergentes. También busca contribuir a la soberanía tecnológica de la UE y a su autonomía estratégica abierta en el ámbito de la ciberseguridad, especialmente al fomentar la innovación en el mercado único digital.

Para alcanzar estos objetivos, el reglamento promueve la solidaridad a escala europea, consolida el ecosistema de ciberseguridad y mejora la ciberresiliencia de los Estados miembros. Mediante el desarrollo de capacidades, conocimientos técnicos, habilidades y competencias de la fuerza laboral en materia de ciberseguridad.

En particular, el Reglamento modifica el **Reglamento (UE) 2021/694**[26] en lo que respecta a la adición de **nuevos objetivos** operativos relacionados con el **Sistema Europeo de Alerta de Ciberseguridad** y el **Mecanismo de Emergencia** en materia de Ciberseguridad en el marco del objetivo 3 del Programa Europa Digital, cuya finalidad es garantizar la resiliencia, la integridad y la fiabilidad del mercado único digital, reforzar las capacidades para seguir los ciberataques y ciberamenazas y responder a ellos, y reforzar la cooperación y la coordinación transfronterizas en materia de ciberseguridad.


W
E
D
C
S
X
Alt
Q
A
Z

05

Autoridades competentes en Ciberseguridad

Autoridades en la UE

La Agencia de la Unión Europea para la Ciberseguridad (ENISA)

Se define como la Agencia de la Unión que se dedica a lograr un alto nivel común de ciberseguridad en todo el territorio europeo. Creada en 2004 y reforzada por la **Ley de Ciberseguridad de la UE**[27], contribuye a la política sobre ciberseguridad, la optimización de la fiabilidad de los servicios y procesos de las tecnologías de la información y la comunicación con esquemas de certificación de ciberseguridad, cooperación con los Estados y los organismos de la Unión, y ayuda a Europa en la preparación de los restos y desafíos del ciberespacio.

Gracias al intercambio de conocimientos, el desarrollo de capacidades y la sensibilización, lleva a cabo la colaboración con sus principales partes interesadas a fin de fortalecer la confianza en la economía conectada, el impulso de la resiliencia de las infraestructuras de la UE y el mantenimiento de la seguridad digital de la sociedad y de la ciudadanía europea.

Estructura y organización

De acuerdo con lo dispuesto en el **Reglamento (UE) 2019/881**, la agencia se compone de los siguientes organismos:

- **Consejo de Administración:** Vela por que la Agencia cumpla sus funciones en condiciones que le permitan operar de manera eficaz de conformidad con lo dispuesto en la Ley de Ciberseguridad.
- **Junta Ejecutiva:** prepara las decisiones que adopta el consejo de administración.
- **Director Ejecutivo:** Se determina como el responsable de la gestión de la agencia y lleva a cabo sus correspondientes funciones de forma independiente.
- **Red Nacional de Oficiales de Enlace:** Facilitan el intercambio de información entre ENISA y los Estados miembros que forman la Unión Europea.
- **Grupo Asesor:** Asiste a ENISA en cuanto al desarrollo de su programa de trabajo, la consecución de los objetivos estratégicos y comunicación con las principales partes interesadas.

Medios económicos

Entre 2005 y 2009, contó con un presupuesto de 32 millones de euros. Su mandato se amplió hasta 2012 con una dotación anual de 8 millones, que en 2018 ascendió a 11,4 millones.

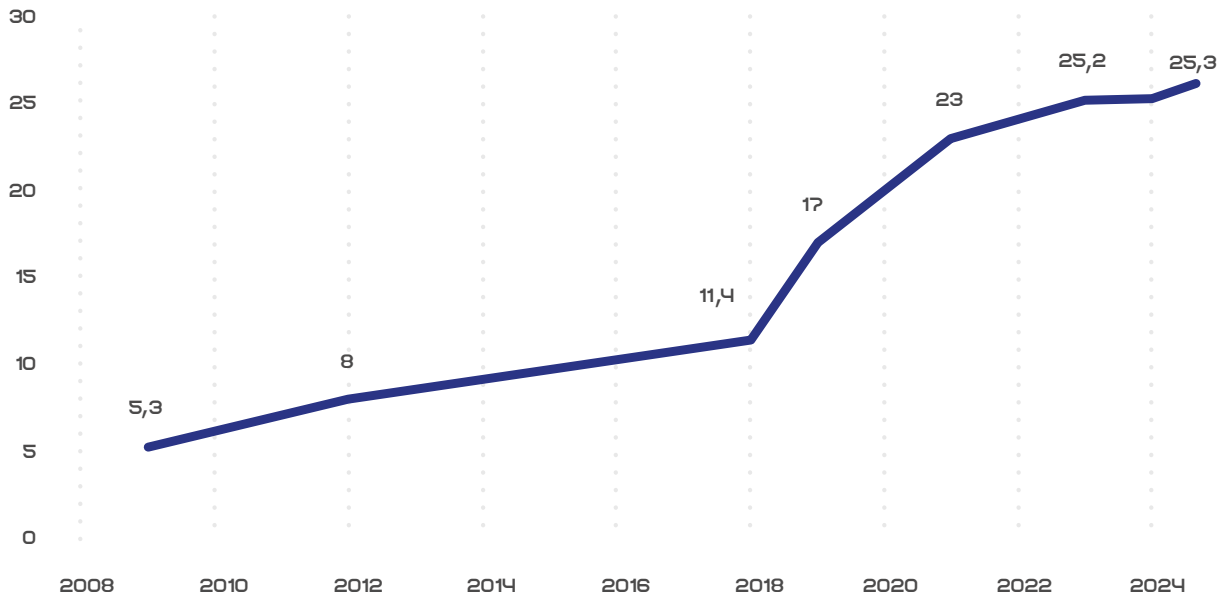
En 2019, la cifra se eleva a 17 millones, y en 2021 alcanza los 23 millones. Ese mismo año, la plantilla pasó de 84 a 125 personas, según los últimos datos oficiales.

ENISA coordina certificación, cooperación y capacidades para reforzar la ciberseguridad común en la UE

El último balance disponible, de 2024, refleja un presupuesto de 25,3 millones de euros. La Agencia se financia con cargo al presupuesto de la UE y con aportaciones de terceros países que participan en sus actividades.

El presupuesto de ENISA es de 25,3 millones

Figura 1.
Presupuesto ENISA en millones de euros



Los **gastos** de la agencia incluyen el personal, la administración y las infraestructuras, así como los gastos operativos relacionados con las actividades de la agencia, al ser el **director ejecutivo** la figura que ejecuta el presupuesto de la agencia.

Capacidades y competencia

En concreto, ENISA apoya a las autoridades nacionales a través del desarrollo de mecanismos como el **Marco de Capacidades en Ciberseguridad**, que es una estructura diseñada para evaluar y mejorar las capacidades nacionales de ciberseguridad, y actúa como una referencia para medir y reforzar dichas capacidades.

Asimismo, realiza ejercicios específicos y programas de formación para desarrollar conocimientos especializados, mejorar las capacidades prácticas y ayudar a reforzar la cooperación nacional y transfronteriza en materia de ciberseguridad.

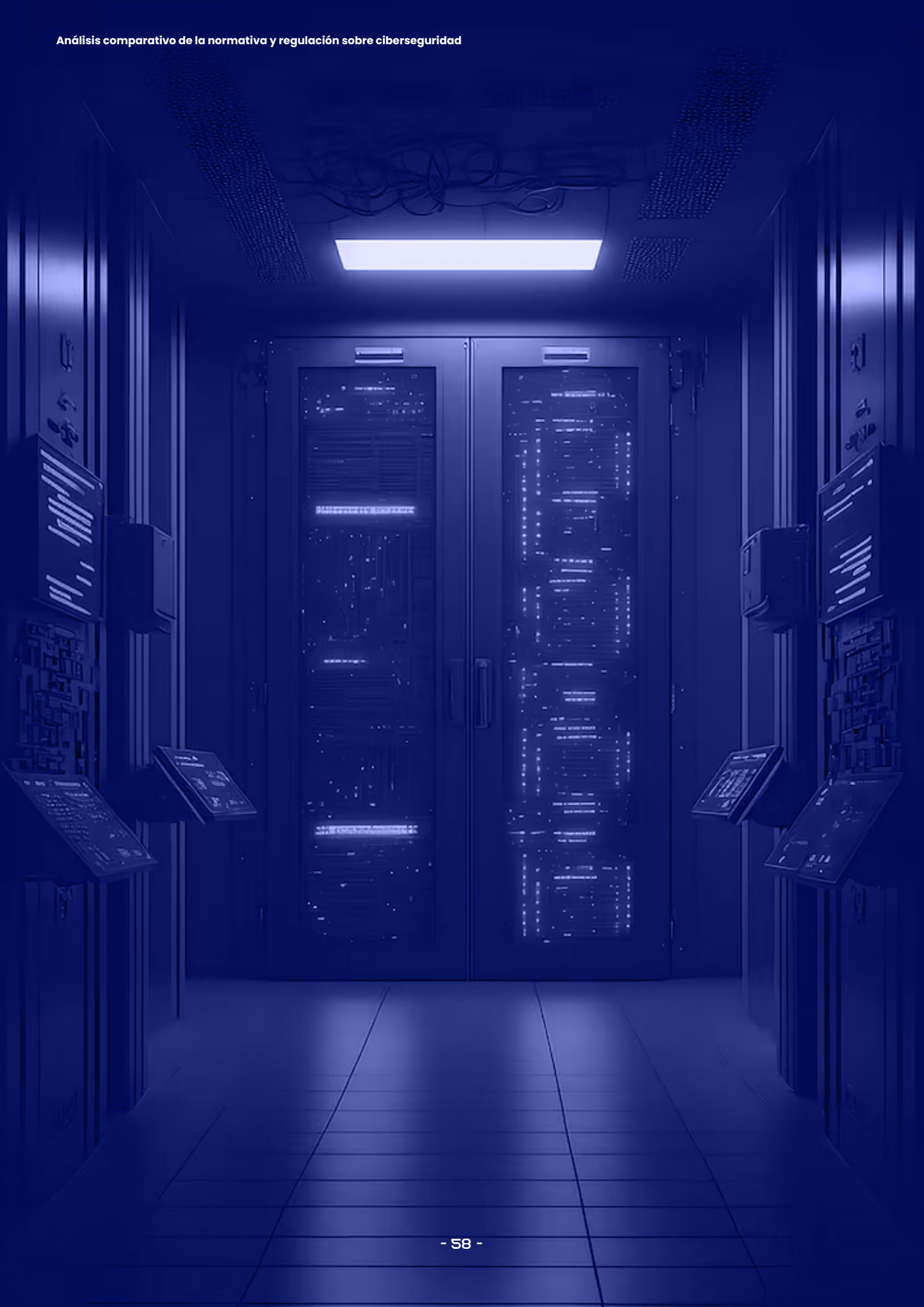
De conformidad con el **artículo 18 de la Directiva 2022/2555**[28] , ENISA, junto con la Comisión Europea y el Grupo de Cooperación, elabora un informe bienal sobre el estado de la ciberseguridad en la Unión Europea.

El informe ofrece a los responsables políticos una visión general basada en datos sobre el contexto y las capacidades de ciberseguridad en los ámbitos europeo, nacional y social. A partir de este análisis se formulan recomendaciones para corregir las deficiencias detectadas y reforzar el nivel de ciberseguridad en la Unión Europea.

Transparencia

La Agencia cumple su compromiso con la **transparencia** por medio de la publicación de documentos sobre los procedimientos de ENISA, su declaración de intereses, su compromiso con el Código de buena conducta administrativa, incluido su programa de trabajo anual y las actas de las reuniones de su Consejo de Administración.

La publicación de los procedimientos le permite presentar y proporcionar a la ciudadanía una visión global del funcionamiento interno y del entorno de la Agencia.



Autoridades en España

Seguridad Nacional

La **Seguridad Nacional en España** es una responsabilidad y función compartida por diversas entidades y organismos gubernamentales que trabajan de manera coordinada entre ellos para prevenir y responder a amenazas internas y externas.

A continuación, se detallan las entidades y organismos responsables de la Seguridad Nacional en España junto a su organización y estructura, y se centra en aquellas relevantes en el ámbito de la ciberseguridad.

El **Sistema de Seguridad Nacional**, es el conjunto de órganos, organismos, recursos y procedimientos que permite a los órganos competentes en materia de Seguridad Nacional ejercer sus funciones, según recoge la Ley 36/2015[29]. A continuación, se detallan los niveles de coordinación y actuación por los que está compuesto:

- El Presidente del Gobierno es la máxima autoridad en materia de Seguridad Nacional y el encargado de coordinar la acción del país en este ámbito.
- El Consejo de Seguridad Nacional es el órgano colegiado que asiste al Presidente en materia de Seguridad Nacional y ejerce las funciones que se le atribuyan en la Ley de Seguridad Nacional.
- El Departamento de Seguridad Nacional (DSN) es el órgano de asesoramiento al presidente del Gobierno en materia de Seguridad Nacional.
- Comités especializados de apoyo al consejo de seguridad nacional en áreas específicas. este grupo lo componen nueve comités entre los que se encuentra el consejo nacional de ciberseguridad, un órgano colegiado de apoyo al consejo que refuerza las relaciones de coordinación, colaboración y cooperación entre las distintas administraciones públicas con competencias en materia de ciberseguridad. conforman el consejo nacional de ciberseguridad: el centro nacional de inteligencia (CNI), el departamento de seguridad nacional (DSN) y los siguientes organismos:

- Ministerio de Asuntos Exteriores, UE y Cooperación
- Ministerio de Defensa
- Ministerio del Interior
- Ministerio de Trabajo y Economía Social
- Ministerio para la Transición Ecológica y el Reto Demográfico
- Ministerio de Sanidad
- Ministerio para la Transformación Digital y de la Función Pública
- Ministerio de la Presidencia, Justicia y Relaciones con las Cortes
- Ministerio de Hacienda
- Ministerio de Transportes y Movilidad Sostenible
- Ministerio de Industria y Turismo
- Ministerio de Economía, Comercio y Empresa
- Ministerio de Ciencia, Innovación y Universidades
- Otros ministerios de Educación, Formación Profesional y Deportes

Todos se reúnen a iniciativa del Presidente del Gobierno, como mínimo, con carácter bimestral o cuantas veces lo considere necesario atendiendo a las circunstancias que afecten a la Ciberseguridad.

Según la estructura y composición del **Sistema de Seguridad Nacional**, este es el órgano del **Consejo de Seguridad Nacional**.

Los componentes del Consejo de Seguridad Nacional se establecen en la Ley de Seguridad Nacional[29] y, a fecha del presente informe, los ministerios que, como mínimo, lo integran son los siguientes, cuyos nombres se indican actualizados conforme a su denominación oficial vigente:

- Presidente del Gobierno.
- Las Vicepresidentas o vicepresidentes del Gobierno, si los hubiere.
- Los Ministros o ministras de Asuntos Exteriores, Unión Europea y de Cooperación, de Presidencia, Justicia y Relaciones con las Cortes, de Defensa, de Hacienda, del Interior, de Transportes y Movilidad Sostenible, de Industria

y Turismo, de Economía, Comercio y Empresa, de Sanidad, de Transformación Digital y Función Pública, de Trabajo y Economía Social, de Ciencia, Innovación y Universidades.

- El director o directora del Gabinete de la Presidencia del Gobierno, el Secretario o secretaria de Estado de Asuntos Exteriores, la jefa o el Jefe de Estado Mayor de la Defensa, el Secretario o Secretaria de Estado de Seguridad y el Secretario o Secretaria de Estado-Director o Directora del CNI.
- Director o directora del Departamento de Seguridad Nacional.

También podrán formar parte del Consejo, cuando sean convocados en función de los asuntos a tratar, los titulares de los demás departamentos ministeriales y las autoridades autonómicas afectadas en la toma de decisiones y actuaciones a desarrollar por parte del Consejo.

A continuación, se presenta una selección de los ministerios que, al formar parte del Consejo de Seguridad Nacional, disponen de una entidad o área específica cuya competencia está dedicada de manera exclusiva a la ciberseguridad.

Ministerio	Entidad/Área dedicada a Ciberseguridad
Ministerio del Interior	Oficina de Coordinación de Ciberseguridad (OCC)
Ministerio de Defensa	Mando Conjunto del Ciberespacio (MCCE)
Ministerio de la Presidencia, Justicia y Relaciones con las Cortes	Subdirección General de Calidad de los Servicios Digitales, Ciberseguridad y Operaciones
Ministerio de Hacienda	Centro de Ciberseguridad y Protección de Datos de la Agencia Tributaria
Ministerio para la Transformación Digital y de la Función Pública	Instituto Nacional de Ciberseguridad (INCIBE)

Tabla 1.
Ministerios del Consejo de Seguridad Nacional con entidades dedicadas a Ciberseguridad

Ministerio del Interior

Órgano del Gobierno de España al que le corresponde el mando superior de las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE), la dirección de las competencias del Ministerio en materia de la administración penitenciaria, así como las demás competencias y atribuciones que le confiere el ordenamiento jurídico.

El órgano superior del Ministerio del Interior, encargado de coordinar las FFCCSE y la seguridad pública, es la **Secretaría de Estado de Seguridad (SES)**.

Sus organismos clave son:

- **Dirección General de la Policía (DGP)**
  Responsable de la ordenación, dirección, coordinación y ejecución de las misiones que a la Policía Nacional encomienden las disposiciones vigentes. La **Brigada Central de Investigación Tecnológica** es la Unidad policial destinada para responder frente los incidentes de ciberseguridad, encuadrada en la Unidad de Investigación Tecnológica.

  Asume la investigación y persecución de las actividades delictivas que impliquen la utilización de las tecnologías de la información y las comunicaciones (TIC) y el ciberdelito de ámbito nacional y transnacional.

- **Dirección General de la Guardia Civil (DGGC)**
  Responsable de la ordenación, dirección, coordinación y ejecución de las misiones que a la Guardia Civil encomienden las disposiciones vigentes. Se encuentra el **Grupo de Delitos Telemáticos (GDT)**, creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos actos delictivos que se cometen a través de sistemas de telecomunicaciones y mediante las tecnologías de la información.

- **Dirección General de Coordinación y Estudios**
  Encargada de impulsar, coordinar y supervisar, a través del **Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)** todas las actividades que tiene encomendadas la Secretaría de Estado en relación con la protección de las infraestructuras críticas y de los servicios esenciales en el territorio nacional, en colaboración con otros departamentos ministeriales.

  Además, a través de la **Oficina de Coordinación de Ciberseguridad (OCC)**, actúa de punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros relativa a los ciberataques contra los sistemas de información, ejerce como canal específico de comunicación entre los Centros de Respuesta a Incidentes Cibernéticos (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad y se constituye como el Centro de Respuesta a Incidentes Cibernéticos del Ministerio del Interior en apoyo a la Policía Judicial **(CSIRT-MIR-PJ)**.

  Este centro refuerza la capacidad del Ministerio del Interior para prevenir, detectar y responder a ciberataques, al mejorar la coordinación entre las unidades de investigación de la Policía Nacional y la Guardia Civil.

Ministerio de Defensa

Órgano del Gobierno de España responsable de la defensa nacional y las Fuerzas Armadas (FAS). De acuerdo con el Real Decreto 205/2024[30], de 27 de febrero, se estructura en los siguientes órganos superiores:

- **Estado Mayor de la Defensa**
  Órgano encargado de preparar la fuerza, promulgar la doctrina militar nacional y establecer la Fuerza Conjunta. Le corresponde, entre otras funciones, el desarrollo y detalle de las políticas de seguridad de la información en los sistemas de información y telecomunicaciones, así como la dirección de la ejecución y el control del cumplimiento de estas normas.

  Del Estado Mayor de la Defensa depende el **Mando Conjunto del Ciberespacio (MCCE)**, órgano responsable de definir, dirigir y coordinar la concienciación, formación y adiestramiento en materia del ciberespacio.

  Entre sus competencias están realizar las acciones necesarias para garantizar

la supervivencia de los elementos físicos, lógicos y virtuales críticos para la Defensa y las FAS, ejecutar operaciones militares en el ciberespacio. Contribuir a la ciberinteligencia militar, colaborar con otros organismos como CCN u OTAN en materia de ciberseguridad y ciberdefensa e impulsar la capacitación y el entrenamiento en ciberdefensa dentro de las FAS.

El MCCE incluye el Equipo de Respuesta ante Emergencias Informáticas del Ministerio de Defensa, **ESPDEF-CERT**, responsable de las entidades con incidencia en la Defensa Nacional. Su ámbito de actuación son las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y afecten a la defensa nacional.

- **Centro Nacional de Inteligencia**

Además, está adscrito al Ministerio de Defensa, con dependencia directa de la persona titular del Departamento, el **Centro Nacional de Inteligencia (CNI)**, organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o la integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones.

El CNI es la **máxima autoridad** de la inteligencia y seguridad del país y sus competencias se rigen por la Ley 11/2022[31], entre ellas se encuentra la recopilación y análisis de información relacionada con la seguridad nacional, la prevención de amenazas en este ámbito mediante su identificación, análisis y evolución, la coordinación de otros servicios de inteligencia y organismos de seguridad, colaboración internacional en la lucha de amenazas transnacionales y garantizar la protección de los sistemas de información e infraestructuras críticas frente a ciberataques.

Perteneciente al CNI, se encuentra el organismo del **Centro Criptológico Nacional (CCN)**, encargado de garantizar la ciberseguridad en los diferentes organismos de la Administración Pública y otros sectores estratégicos y de dar respuesta a las funciones planteadas en el Real Decreto 421/2004, de 12 de marzo[32].

Entre estas funciones se incluye la elaboración y difusión de normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas TIC, conocidas como **Guías CCN-STIC**. Estas guías son actualizadas y completadas de manera periódica, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT.

El grueso de las series está especialmente dirigido al personal de las Administraciones Públicas y empresas y organizaciones de interés estratégico y otras de difusión pública para todas las personas usuarias. El CCN también es responsable de formar, sensibilizar y asesorar a las Administraciones Públicas en materia de ciberseguridad.

Además, el CCN es un organismo de vital importancia ya que entre sus responsabilidades se incluye la contribución a la mejora de la ciberseguridad española a través del **CCN-CERT**. Se trata del equipo de respuesta a incidentes del CCN y su función es ser el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

De acuerdo con la Ley 40/201536, es competencia del CCN-CERT la gestión de incidentes de ciberseguridad que afecten a cualquier organismo o empresa pública.

Por último, el CCN es el responsable de gestionar el **Esquema Nacional de Seguridad (ENS)** y de constituir el Organismo de Certificación (OC) del mismo. El CCN es la autoridad de referencia en materia de ENS, encargada de la elaboración y mantenimiento de la normativa técnica complementaria del ENS, su supervisión y apoyo a la implantación, así como de la validación de auditorías del ENS.

Ministerio de Justicia

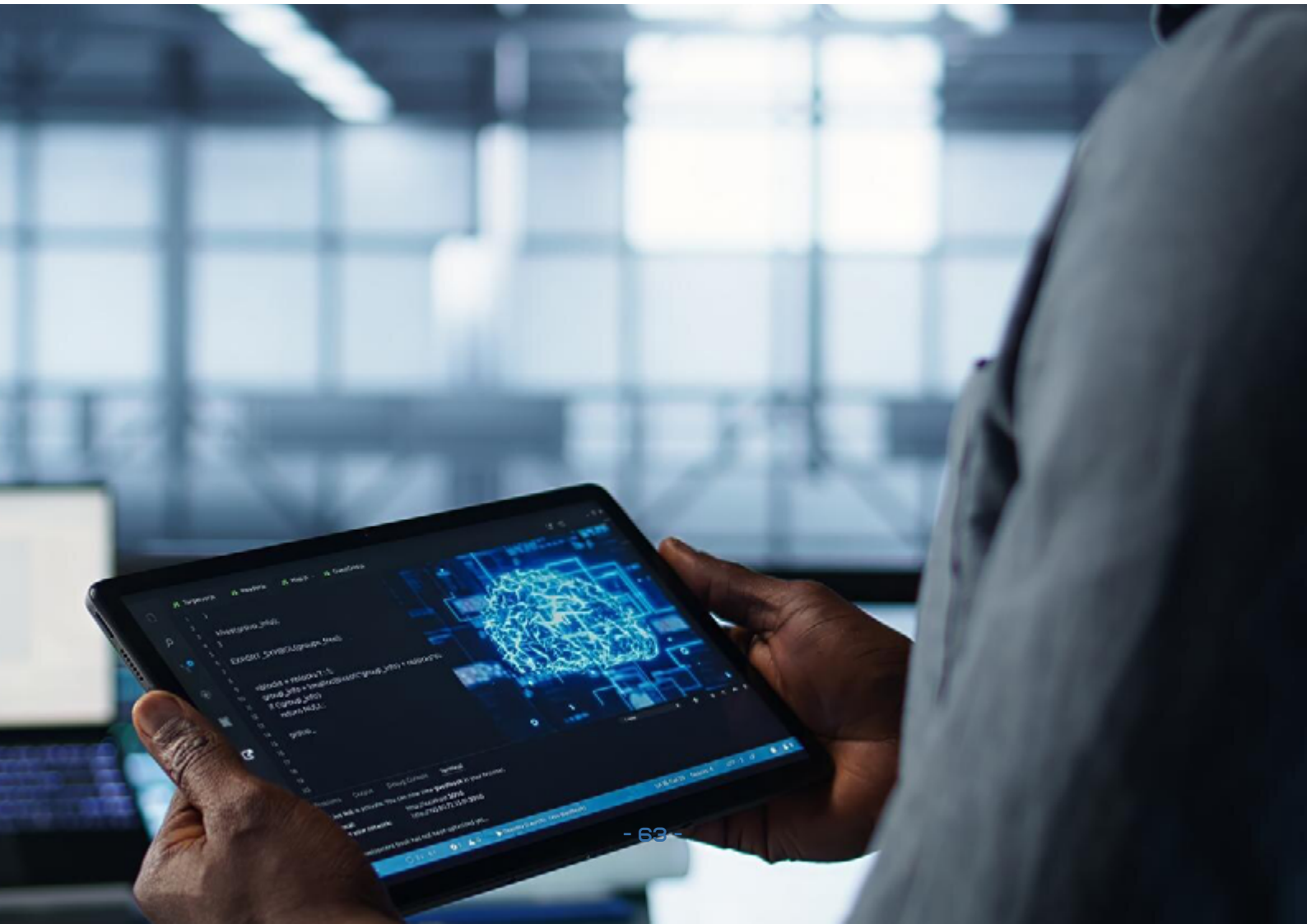
Órgano del Gobierno de España responsable de la coordinación de los asuntos de relevancia constitucional, así como la preparación, desarrollo y seguimiento del programa legislativo. Correspondiente a su estructura, se encuentra la **Subdirección General de Calidad de los Servicios Digitales, Ciberseguridad y Operaciones**, perteneciente a la Dirección General de Transformación Digital de la Administración de Justicia (DGTDAJ), bajo la dirección de la Secretaría General para la Innovación y Calidad del Servicio Público de Justicia.

Tiene como objetivo principal liderar el cambio cultural y tecnológico para la modernización de la Administración de Justicia, así como la provisión de servicios de tecnologías de la información y comunicación de las Gerencias Territoriales y el mantenimiento operativo y creación de soluciones tecnológicas.

Dependiente del Ministerio de Justicia, se encuentra la **Agencia Española de Protección de Datos (AEPD)**, oque vela por el cumplimiento de la normativa de protección de datos y controlar su aplicación, aprobada y definida en el Real Decreto 389/2021[33].

Dentro de sus competencias, garantiza el cumplimiento del Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), ejerce funciones de control e inspección y lleva a cabo investigaciones en forma de auditorías de protección de datos, emite recomendaciones y directrices en materia de protección de datos a organismos tanto públicos como privados.

Además, atiende las reclamaciones de la ciudadanía en este aspecto y promueve la concienciación a través de códigos de conducta, certificaciones y mecanismos de autorregulación.



El Ministerio para la Transformación Digital impulsa la ciberseguridad en España a través del INCIBE

Ministerio para la Transformación Digital y de la Función Pública

Órgano del Gobierno de España al que corresponde la propuesta y ejecución de la política del Gobierno en materia de telecomunicaciones, sociedad de la información, transformación digital y el desarrollo y fomento de la IA.

Asimismo, corresponde al Ministerio para la Transformación Digital y de la Función Pública la propuesta y ejecución de la política del Gobierno en materia de administración pública, función pública y gobernanza pública.

Bajo la dirección de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, se encuentra el **Instituto Nacional de Ciberseguridad (INCIBE)**, organismo público encargado de afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España. Su actividad se basa en la investigación, prestación de servicios y coordinación con los agentes con competencias en la materia.

Sus competencias son garantizar la seguridad en el ciberespacio, y promover la protección de la ciudadanía, las empresas y los operadores de servicios esenciales. Una misión esencial del INCIBE es el desarrollo y promoción de un ecosistema de ciberseguridad a través de programas e iniciativas para la formación, concienciación y sensibilización a la ciudadanía en este ámbito.

También participa en el desarrollo normativo y técnico en materia de seguridad TIC, proporciona apoyo a pymes y grandes empresas en la mejora de su resiliencia digital y colabora activamente con organismos internacionales para hacer frente a las ciberamenazas globales. Perteneciente a INCIBE, se incluye la gestión de incidentes de ciberseguridad a través del **INCIBE-CERT**, centro de respuesta a incidentes de seguridad de referencia para la ciudadanía y entidades de derecho privado en España.

Además, el INCIBE es el **Centro de Coordinación Nacional (NCC-ES)** en España dentro del Centro Europeo de Competencia en Ciberseguridad (ECCC), una iniciativa europea que tiene el objetivo de crear una red europea de Centros Nacionales de Coordinación, constituida por 27 centros, uno por cada Estado, según recoge el Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo[34].

Ministerio de Hacienda

Órgano del Gobierno de España encargado de gestionar las políticas económicas, financieras y fiscales del país. Dentro de su estructura, se encuentra el Departamento de Informática Tributaria, responsable de la gestión tecnológica de la Agencia Estatal de Administración Tributaria (AEAT). Bajo la dependencia directa de su dirección, se encuentra el **Centro de Ciberseguridad y Protección de Datos**.

Desempeña funciones clave como la definición, implantación y mantenimiento de planes de recuperación ante fallos tecnológicos, el desarrollo de procedimientos operativos de seguridad física y lógica, la actualización del registro de funcionarios habilitados para la identificación electrónica de la ciudadanía, la gestión de identidades y credenciales del personal.

Así como la promoción de iniciativas de formación y concienciación en ciberseguridad y protección de datos, la certificación de trámites electrónicos realizados en la Sede Electrónica para garantizar su validez legal, especialmente en procesos tributarios en línea; y la gestión del centro de operaciones de ciberseguridad para monitorizar, evaluar y responder ante amenazas.

Ciberseguridad

De acuerdo con el **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad**[35], elaborado por el Ministerio del Interior y aprobado el 14 de enero de 2025, el punto de contacto único para la ciberseguridad en España es el **Centro Nacional de Ciberseguridad**.

Según recoge el artículo 6, el Centro Nacional de Ciberseguridad ejercerá como Autoridad Nacional de gestión de crisis y punto de contacto único, y asumirá la superior dirección y coordinación de las autoridades de control y puntos de contacto sectoriales en el desarrollo de sus funciones de ejecución y supervisión, así como de los CSIRT nacionales de referencia.

Además, el **Centro Nacional de Ciberseguridad** se constituye como punto de contacto único para ejercer una función de enlace que garantice la cooperación transfronteriza con las autoridades pertinentes en otros Estados miembros y, cuando proceda, con la Comisión y la Agencia de la UE para la Ciberseguridad, así como para garantizar la cooperación intersectorial con otras autoridades competentes nacionales.

El anteproyecto designa a varias **autoridades de control** responsables de supervisar y ejecutar cuestiones de ciberseguridad:

- **Ministerio de Defensa, a través del Centro Criptológico Nacional**, para las entidades esenciales e importantes que, sin ser entidades críticas, se encuentren comprendidas en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre[36].

- **Ministerio para la Transformación Digital y de la Función Pública**, a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y la Secretaría de Estado de Digitalización e Inteligencia Artificial, para las entidades esenciales e importantes de los sectores de infraestructura digital y proveedores de servicios digitales, así como de las entidades importantes del resto de sectores, que no se hayan designado como entidades críticas.

- **Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad de la Secretaría de Estado de Seguridad**, para las entidades críticas y para las entidades esenciales de los sectores no incluidos en los Ministerios de Defensa y Ministerio para la Transformación Digital y de la Función Pública, así como para todas las entidades esenciales e importantes del sector de seguridad privada.

En el artículo 9 del Anteproyecto de Ley se designan los **equipos de respuesta a incidentes de ciberseguridad (CSIRT)** nacionales de referencia:

- El **CCN-CERT**, del Centro Criptológico Nacional (CCN), al que corresponde la comunidad de referencia constituida por las entidades consideradas esenciales o importantes de acuerdo con esta Ley que se encuentren incluidas dentro del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

En todo caso, el CCN-CERT, siguiendo las instrucciones del Centro Nacional de Ciberseguridad, ejercerá la coordinación nacional de la respuesta técnica de los CSIRT en incidentes significativos o supuestos de especial gravedad.

- El **INCIBE-CERT**, operado por el INCIBE, opera como el centro de referencia para la gestión de incidentes de seguridad dirigidos a ciudadanía y entidades de derecho privado en España. Acorde al Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, se encuentra conjuntamente operado por INCIBE y OCC, Oficina de Coordinación de Ciberseguridad del Ministerio del Interior.

El INCIBE-CERT es el organismo al que corresponde la comunidad de referencia constituida por las entidades consideradas esenciales o importantes de acuerdo con esta Ley y que no se encuentren incluidas en el ámbito subjetivo de aplicación de la Ley 40/201536, de 1 de octubre.

• El **ESPDEF-CERT**, del mando conjunto del ciberespacio, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran y, necesariamente, en las relativas a incidentes de entidades con incidencia en la Defensa Nacional, en cuyo caso se coordinarán con él aquellos aspectos que pueda afectar a la Defensa Nacional, al Ministerio de Defensa o a la Operatividad de las Fuerzas Armadas.

Además, apoya a los operadores de servicios esenciales, especialmente aquellos con incidencia en la Defensa Nacional, según lo estipulado reglamentariamente. Este organismo refuerza la capacidad de respuesta de ciberseguridad en el ámbito militar y de defensa estratégica de España

• En los incidentes que afecten a entidades catalogadas como críticas, el **CSIRT-MIR-PJ** de la Oficina de Coordinación de Ciberseguridad (OCC) operará conjuntamente con el CSIRT de referencia correspondiente.

• La **Agencia Española de Protección de Datos (AEPD)** es la responsable de cualquier incidente que afecte a datos personales. Conforme al Anteproyecto "las autoridades de control cooperarán estrechamente con la AEPD y, en su caso, con las autoridades independientes de control de las Comunidades Autónomas, para hacer frente a los incidentes que produzcan violaciones de la seguridad de datos personales, y las informará sobre aquellos incidentes que puedan comprometer la seguridad de los datos personales que deban ser objeto de notificación, y su evolución".

• Según el Real Decreto 43/2021, de 26 de enero[37], el **Banco de España (BE)** desempeña un papel crucial en el ecosistema de ciberseguridad del **sector financiero**, y actúan como regulador, supervisor y coordinador.

Su **función** en este ámbito se centra en garantizar que las entidades financieras y otras instituciones bajo su supervisión gestionen adecuadamente los riesgos de ciberseguridad y cumplan con las normativas aplicables.

El BE colabora con otros organismos nacionales, como el CCN-CERT, el INCIBE-CERT, y el CNPIC, para garantizar una respuesta coordinada a los incidentes de ciberseguridad que puedan tener un impacto sistémico. Según el **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad**, el Banco de España continuará y mantendrá las competencias y funciones que tiene asignadas.

Mientras que las autoridades de control y CSIRTs de referencia deberán informar a la Secretaría de Estado de Economía y Apoyo a la Empresa, del Ministerio de Economía, Comercio y Empresa, sobre aquellos incidentes que tengan efectos significativos en los servicios esenciales del sistema financiero.

A continuación, se presenta un esquema organizativo elaborado a partir de un análisis y mapeo efectuado entre las autoridades de control, conforme a lo establecido en el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad y los organismos contemplados en la Ley de Seguridad Nacional, pertenecientes al Consejo de Seguridad Nacional.

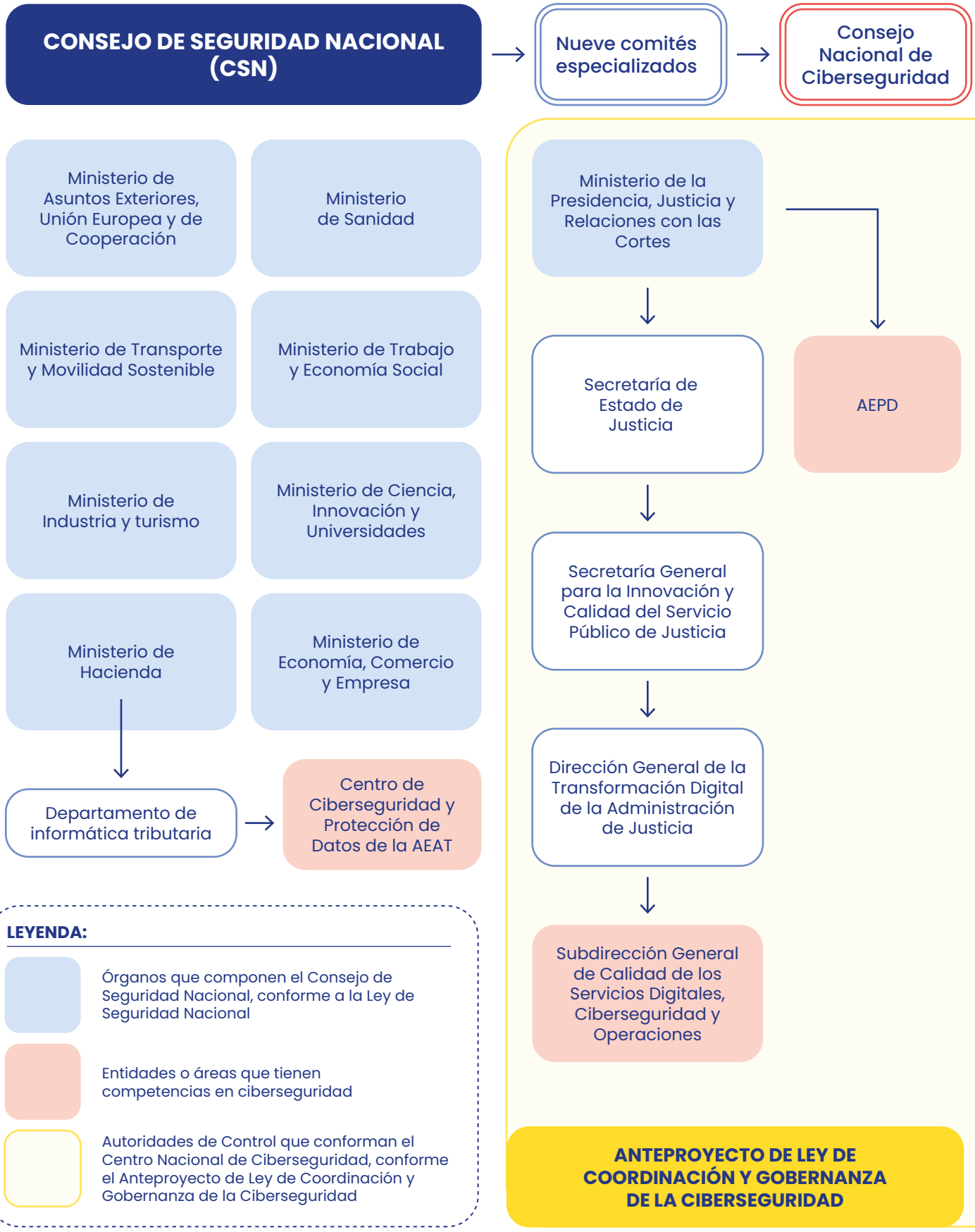
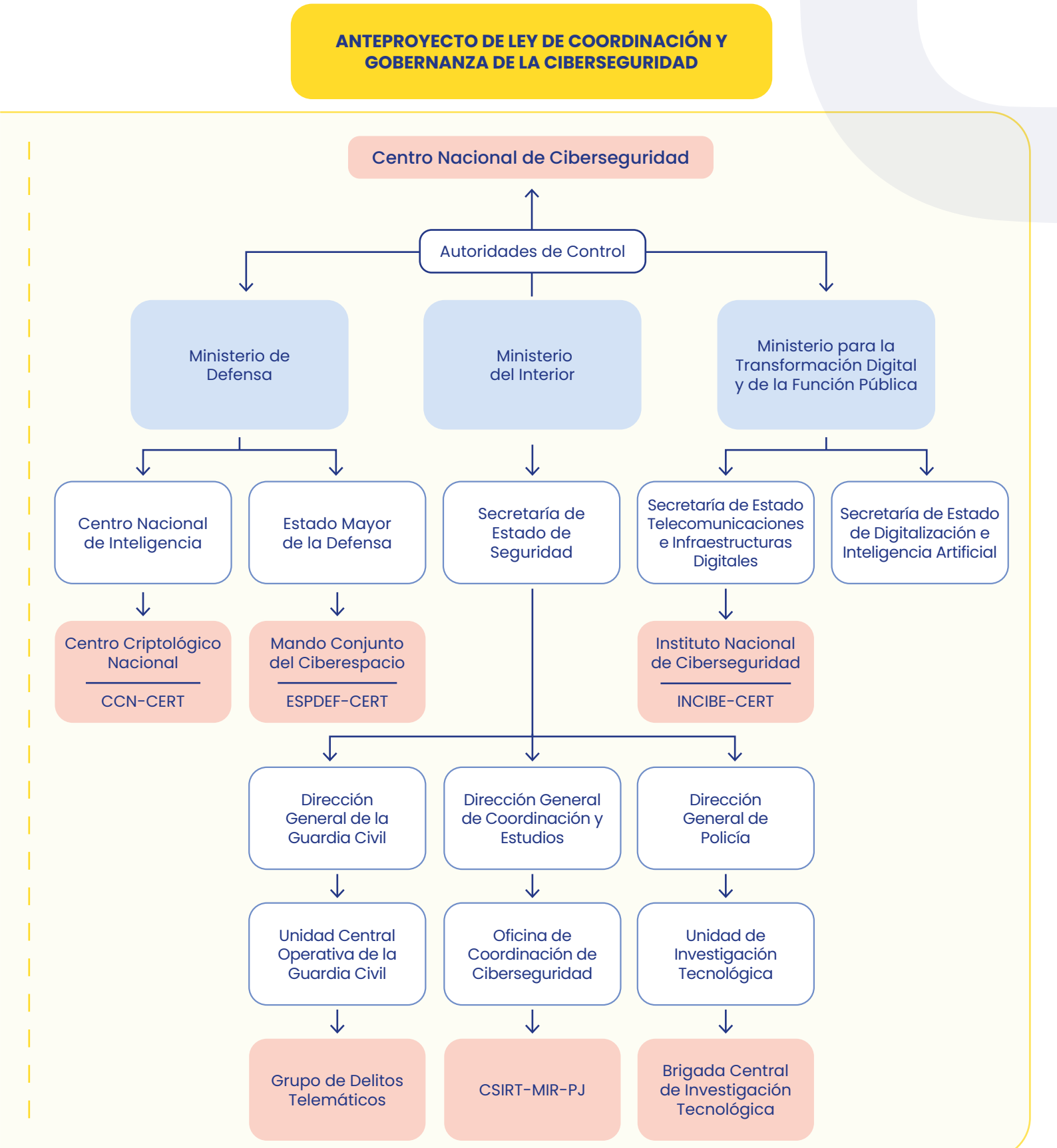


Figura 2.
Esquema organizativo entre autoridades de control del anteproyecto de ley y organismos del Consejo de Seguridad Nacional



06

Gestión de riesgos en ciberseguridad

El nivel de riesgo se determina como una estimación de lo que puede ocurrir y su valoración, de forma cuantitativa, como el producto del impacto, asociado a una amenaza, por la probabilidad de la misma[38].

Impacto x Probabilidad = Riesgo

Figura 3.
Cálculo del riesgo

El **impacto**[xvi], y por tanto el **riesgo**, se valoran en términos del coste derivado del valor de los activos afectados y se consideran, además, de los daños producidos en el propio activo:

- Daños personales.
- Pérdidas financieras.
- Interrupción del servicio.
- Pérdida de imagen y reputación.
- Disminución del rendimiento.

En ciertas ocasiones se considera necesario el desarrollo de un **análisis cualitativ**o, es decir, trabajar con magnitudes económicas proporciona a las organizaciones el establecimiento del umbral de riesgo como el nivel máximo del riesgo que la entidad está dispuesta a soportar. Por tanto, la gestión de riesgos debe mantener el nivel del riesgo siempre por debajo del umbral.

De otra parte, el **coste de protección** es lo que supone para las organizaciones tanto los recursos como los esfuerzos que mantienen el nivel del riesgo por debajo del umbral deseado. En consecuencia, las entidades deben concretar el empleo de los recursos necesarios para cumplir con este objetivo.

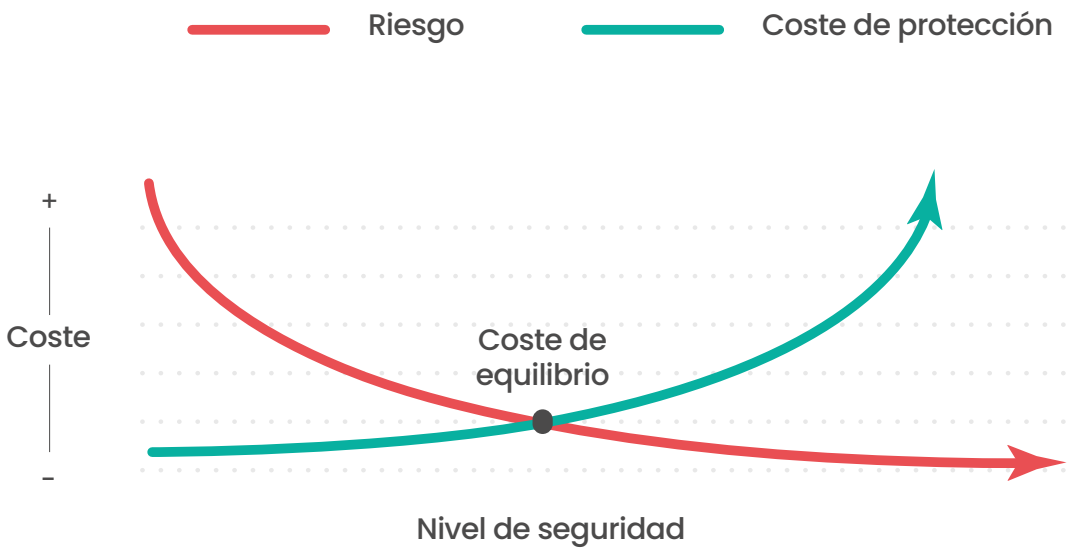


Figura 4.
Coste de equilibrio

En los casos en que las actividades cuyo objetivo es **mantener el riesgo por debajo del umbral fijado** se engloban en los que se determina como la **gestión del riesgo**. Ante ello, las organizaciones que gestionan el riesgo para su actividad deberán de llevar a cabo la realización de:

- **Análisis de riesgo**: Consiste en averiguar el riesgo soportado. Para ello, las distintas metodologías establecen que se realice un inventario de activos, se determinen el elenco de amenazas, las probabilidades de que ocurran y los posibles impactos.
- **Tratamiento de los riesgos:** En caso de que aquellos riesgos se encuentren por encima del umbral deseado, la organización debe decidir cuál es el mejor tratamiento que permita su reducción y mitigación, y pasa por un filtro económico donde el coste del tratamiento, o coste de protección, no supere el coste de riesgo disminuido.

Figura 5.
Gestión de riesgos

Por tanto, el análisis debe ser realizado de manera metódica e impide omisiones, improvisaciones o posibles criterios arbitrarios. En la actualidad, existen diversas metodologías y **guías de buenas prácticas**, tanto generalistas como especializadas, que pueden ser utilizados para desarrollar dicho análisis. Entre las que se destacan:

- **COSO**[39]: Organización americana dedicada a la creación de guías y marcos de trabajo en el ámbito de la gestión de riesgos.
- **ISO 31000:2009**[40]: Norma Global, no certificable, que aporta metodología, principios y directrices en materia de gestión de riesgos.

Específicas para gestión de riesgos de seguridad de la información:

- **MAGERIT**[41]: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información creada por el Ministerio de Administraciones Públicas español.
- **ISO/IEC 27005:2011**[42]: Norma que aporta directrices para la gestión de riesgos de seguridad de la información.
- **NIST SP – 800-30**[43]: Metodología creada en este caso por el gobierno norteamericano.

La UE refuerza la gestión de riesgos de ciberseguridad en las entidades esenciales

Situación en la UE

El entorno y contexto digital europeo se enfrenta a nuevos desafíos en materia de ciberseguridad, a causa de la aparición de **amenazas emergentes** que afectan tanto al sector público, como al privado. Ante ello, la Unión Europea ha llevado a cabo el desarrollo de un marco regulatorio sólido a fin de garantizar la **protección de su infraestructura digital crítica**.

La **Directiva NIS2**[44], junto con el **Reglamento 2024/2690**[45] establece un marco de referencia de carácter obligatorio para las entidades relevantes que se encuentren en la Unión, en donde se implementan la base para proceder a la gestión de riesgos de ciberseguridad en relación con entidades consideradas esenciales, como pueden ser los proveedores de servicios, centro de procesamiento de datos y plataformas de redes sociales.

La gestión de riesgos es un aspecto esencial para reforzar la resiliencia cibernética, por lo que, el presente reglamento no solo determina los riesgos que han de ser objeto de tratamiento, sino que también expone las distintas **metodologías** para llevar a cabo su identificación, análisis y mitigación.

Ha de tenerse en cuenta la **exposición al riesgo** de las entidades que sean pertinentes, en función de su carácter esencial, de los riesgos a los que se encuentren expuestas, de su estructura y tamaño, o de la probabilidad de que ocurran los incidentes y su gravedad, lo que incluye las repercusiones económicas y sociales, en caso de que se cumplan los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos.

De acuerdo con el **principio de proporcionalidad**, cuando las entidades pertinentes no puedan aplicar algún requisito técnico y/o metodológico de las medidas para la gestión de riesgos en materia de ciberseguridad a causa de su tamaño, dichas entidades han de poder adoptar otras medidas compensatorias que se consideren adecuadas para lograr los objetivos de dichos requisitos.

ENISA o las autoridades nacionales competentes contempladas en la **Directiva NIS2** pueden proporcionar orientaciones de apoyo a las entidades en cuanto a la detección, análisis y evaluación de riesgos con la finalidad de llevar a cabo los requisitos técnicos y metodológicos en relación con el establecimiento y mantenimiento de un marco de gestión de riesgos adecuado.

Con la finalidad de **mitigar los riesgos derivados de la cadena de suministro** de la entidad pertinente y de su relación con los distintos proveedores, dicha entidad ha de implantar una política de seguridad de la cadena de suministro por la cual se rija las relaciones con los proveedores y prestadores de servicios directos.

Asimismo, las entidades establecerán, en los determinados contratos con los proveedores y los prestadores de servicios directos, cláusulas en materia de seguridad, en donde se exijan medidas para la gestión de los riesgos de ciberseguridad, de conformidad con el **artículo 21.2 de la Directiva NIS2** u otras normativas vigentes similares.

El Reglamento tiene como **propósito**:

- Estandarizar la aplicación de medidas relativas a la gestión de los riesgos en materia de ciberseguridad en la UE.
- Implementar metodologías y directrices técnicas.
- Favorecer el cumplimiento normativo y la supervisión en cada uno de la Estados miembros a través de las autoridades nacionales competentes.

El documento normativo se estructura en 13 títulos, los cuales se encuentran enfocados en aspectos críticos de la gestión de riesgos y la ciberseguridad:

- Título 1. **Políticas específicas para la seguridad de redes y sistemas**
- Título 2. **Gestión de riesgos**
- Título 3. **Manejo de incidentes**
- Título 4. **Continuidad del negocio y gestión de crisis**
- Título 5. **Seguridad en la cadena de suministro**
- Título 6. **Adquisición, desarrollo y mantenimiento seguros**
- Título 7. **Evaluación de medidas de gestión de riesgos**
- Título 8. **Prácticas básicas de higiene cibernética y formación**
- Título 9. **Cifrado**
- Título 10. **Seguridad en recursos humanos**
- Título 11. **Control de acceso**
- Título 12. **Gestión de activos**
- Título 13. **Seguridad física y ambiental**

En lo relativo al carácter obligatorio de establecer un **marco de gestión de riesgos**, el cual permita a las pertinentes entidades identificar, evaluar y mitigar amenazas de forma proactiva, dicho marco debe estar integrado en la estrategia de gestión de riesgos de cada entidad, y debe componerse como mínimo de:

1. **Identificación de riesgos**: Evaluación de las amenazas tanto internas como externas, e incluye también los puntos únicos de falla.

2. **Análisis y evaluación**: Definir la probabilidad e impacto de cada riesgo que se haya identificado.

3. **Plan de tratamiento de riesgos**: Implementar el elenco de medidas de seguridad a fin de mitigar o transferir riesgos y llevar a cabo la documentación de los riesgos residuales aceptados.

Asimismo, el reglamento realiza un énfasis en el carácter necesario de un **monitoreo continuo**, por el que se asegure que las medidas sean eficaces y ajustadas.

El **artículo 6.39** de la **NIS2**[46] define a los proveedores y proveedoras de servicios gestionados como: "Una entidad que presta servicios relacionados con la instalación, la gestión, la explotación o el mantenimiento de productos, redes, infraestructuras o aplicaciones de las tecnologías de la información y la comunicación, o cualesquiera otros sistemas de redes y de información (...)." La definición se refiere explícitamente a actividades llevadas a cabo en las instalaciones del cliente o a distancia. Cada una de estas tareas (instalación, gestión, explotación y mantenimiento) no son excluyentes unas de otras, y una entidad puede acometer una o varias de ellas.

Los proveedores de productos y servicios han de cumplir con un elenco de **responsabilidades y obligaciones** en materia de ciberseguridad, en donde se incluyen:

- **Aplicación de medidas relativas a la gestión de riesgos.**
- **Comunicación y/o notificación de incidentes.**
- **Seguridad en la cadena de suministro.**
- **Designación de responsables en la alta dirección.**
- **Planificación sobre la respuesta y recuperación del servicio ante la producción de incidentes.**
- **Cumplimiento de auditorías acorde a la responsabilidad legal.**

Situación en España

La gestión de riesgos de ciberseguridad se encuentra regulada por medio de diferentes normativas que establecen una serie de obligaciones y directrices con la finalidad de proteger las redes y sistemas de información en el país:

• **Anteproyecto de Ley de Coordinación y Gobernanza**[47]: Para reforzar la protección de las redes y sistemas de información que son ya cruciales para el desarrollo de la inmensa mayoría de las actividades sociales y económicas actuales, y que están sometidas a graves ciberamenazas, nuevos desafíos y riesgos que requieren respuestas adaptadas, coordinadas e innovadoras.

El anteproyecto diseña la Estrategia Nacional de Ciberseguridad y crea el Centro Nacional de Ciberseguridad, órgano de contacto único con la UE adscrito a la Secretaría General de Presidencia del Gobierno que se encargará de la dirección, impulso y coordinación en la materia, garantizará la cooperación intersectorial y transfronteriza con otras autoridades competentes y será autoridad de gestión de las crisis de ciberseguridad.

• **Real Decreto 311/2022**[48]: En donde se establecen los requisitos y principios relativos a la política de seguridad en el uso de los medios electrónicos. El Esquema Nacional de Seguridad es obligatorio para todas las entidades públicas y aquellos proveedores que colaboran con ellas. Se lleva a cabo la aplicación de criterios y metodologías de reconocimiento en la materia de la gestión de riesgos y seguridad de las tecnologías de la información y la comunicación.

•**Ley 8/2011**[49]: Implanta un marco de actuación para la protección y la seguridad relativas a las infraestructuras esenciales que garantizan aquellos servicios básicos sociales. Su principal objetivo se centra en la identificación y protección de las dichas infraestructuras ante las amenazas y riesgos, por lo que se asegura de tal forma la continuidad de los servicios esenciales.

• **Ley Orgánica 3/2018**[50]: Aunque se centra en la protección de datos personales, impone obligaciones a los responsables en materia de seguridad de la información y la gestión de los riesgos relativos al tratamiento de datos de carácter personal. Por tanto, según esta normativa, los organismos se encuentran obligados a implantar medidas de seguridad tanto técnicas como organizativas adecuadas para garantizar un nivel de seguridad que se adecúe al riesgo.

Para el tratamiento de riesgos, las entidades nacionales tanto del sector público como el privado cuentan, entre otras, con las siguientes opciones:

•**Evitar o eliminar el riesgo**: Se sustituye el activo por otro que no sea vea afectado por la amenaza o eliminando la actividad que lo produce.

• **Reducirlo o mitigarlo**: Lleva a cabo las medidas oportunas para que el nivel de riesgo se sitúe por debajo del umbral.

•**Transferirlo, compartirlo o asignarlo a terceros**: En aquellos casos en donde la entidad o el organismo no cuente con la capacidad de tratamiento y precisa la contratación de un tercero con capacidad para la reducción y gestión del riesgo y lo deja por debajo del umbral.

• **Aceptarlo**: Se asume el riesgo, bien porque se encuentra debajo del umbral aceptable de riesgo, o bien en casos en que los costes de su tratamiento son muy elevados y aunque son riesgos de impacto alto, su probabilidad de que ocurra es baja.

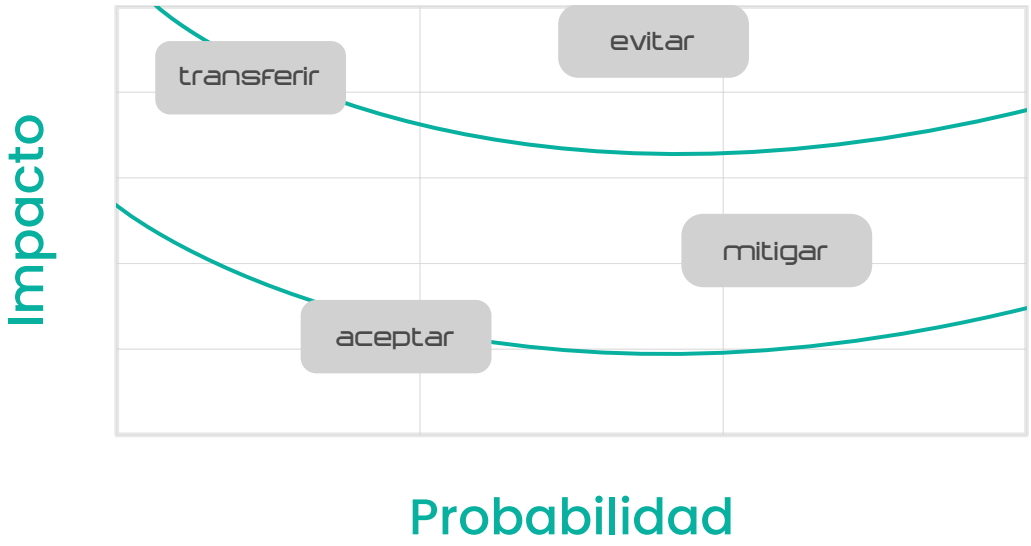


Figura 6.
Opciones del tratamiento de riesgo

El **Real Decreto-ley 12/2018**[51] establece tres **obligaciones** principales para los Proveedores de Servicios:

- Comunicar su actividad a la autoridad competente.
- Adoptar medidas de seguridad técnicas y organizativas adecuadas y proporcionadas.
- Notificar incidentes de seguridad que tengan efectos perturbadores significativos en sus servicios a la autoridad competente a través de su CSIRT de referencia.

Además, el mencionado RD establece en sus **artículos 9.1 y 11.1**, que la autoridad competente y CSIRT de referencia para proveedores de servicios son respectivamente la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital e INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España.

Por ello, conforme al **artículo 7**, los proveedores de servicios deberán: "Comunicar su actividad a la autoridad competente en el plazo de tres meses desde la fecha de su inicio, a los meros efectos de su conocimiento."

Asimismo, dispone en su **artículo 16**, que los proveedores de servicios deberán: "Adoptar las medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información utilizados para la prestación de sus servicios."

Por último, en su **artículo 19.2**, que los proveedores de servicios deberán: "Comunicar a la autoridad competente, a través de su CSIRT de referencia, los incidentes que tengan efectos perturbadores significativos en dichos servicios, considerándose a tal efecto los incidentes con un nivel de impacto crítico, muy alto o alto", según el detalle que se especifica en la guía nacional de notificación y gestión de incidentes de ciberseguridad que figura como anexo en el Real Decreto 43/2021[52].

07
Conclusiones

Principales hallazgos del informe

• Consolidación de la ciberseguridad en el plano europeo y nacional
Aumenta el compromiso para garantizar una eficiente protección cibernética, tanto en la Unión Europea como a nivel nacional, en España. Este se ve plasmado en la implementación y desarrollo de las determinadas estrategias nacionales en materia de ciberseguridad como la Estrategia Nacional de Ciberseguridad en España, y a nivel europeo en políticas de gran consideración como la Estrategia Digital de la UE o la Directiva NIS2[53].

• Desarrollo de la seguridad de los sistemas de información y telecomunicaciones que soportan las Infraestructuras Críticas
Fortalecimiento de la resiliencia de las infraestructuras críticas para evitar una potencial alteración del funcionamiento corriente de los servicios esenciales que podrían afectar a la vida diaria de la ciudadanía. Ante ello, se garantiza la implantación de la normativa sobre protección de las infraestructuras críticas para conseguir una seguridad que conlleve tanto el ámbito físico como el tecnológico.

• Compromiso Internacional
Se puede observar un compromiso internacional en relación con la globalización tecnológica, sus oportunidades y riesgos, que obligan a alinear las iniciativas de la totalidad de los Estado miembros que persiguen un ciberespacio seguro y confiable.

Los esfuerzos internacionales deben contemplar la elaboración y adopción de estándares globales, la expansión de la capacidad del sistema jurídico internacional y el desarrollo y la promoción de las mejores prácticas en el conocimiento de la situación, la alerta y la respuesta ante los incidentes cibernéticos.

• Surgimiento de nuevas amenazas y transformación digital
A partir de la activa digitalización que transforman la estructura y organización de las distintas organizaciones, se impulsa la adopción de las tecnologías emergentes como el internet de las cosas o la inteligencia artificial.

• Relevancia de la cultura en ciberseguridad: formación y capacitación
Concienciar a la ciudadanía, profesionales y empresas de la relevancia e importancia de la ciberseguridad y del uso correcto y responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.

Como presupuesto principal, se desarrolla el impulso de las actividades de sensibilización para garantizar que las personas y organismos tienen acceso a información relacionada con vulnerabilidades, ciberamenazas e información sobre la protección de su entorno tecnológico, así como el desarrollo de programas de concienciación en materia de ciberseguridad.

• Proactividad y capacidad frente a las ciberamenazas

En este contexto, se amplía y mejora la capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas a fin de garantizar la coordinación, cooperación y el intercambio de la información entre los distintos organismos y entidades competentes en la UE.

Asimismo, se lleva a cabo el desarrollo y actualización periódica de las instrucciones de prevención y detección, en donde se incluyen los procesos de respuesta ante las situaciones de crisis y planes de contingencia concretos antes incidentes de ciberseguridad de ámbito nacional y europeo.

• Armonización de normativas

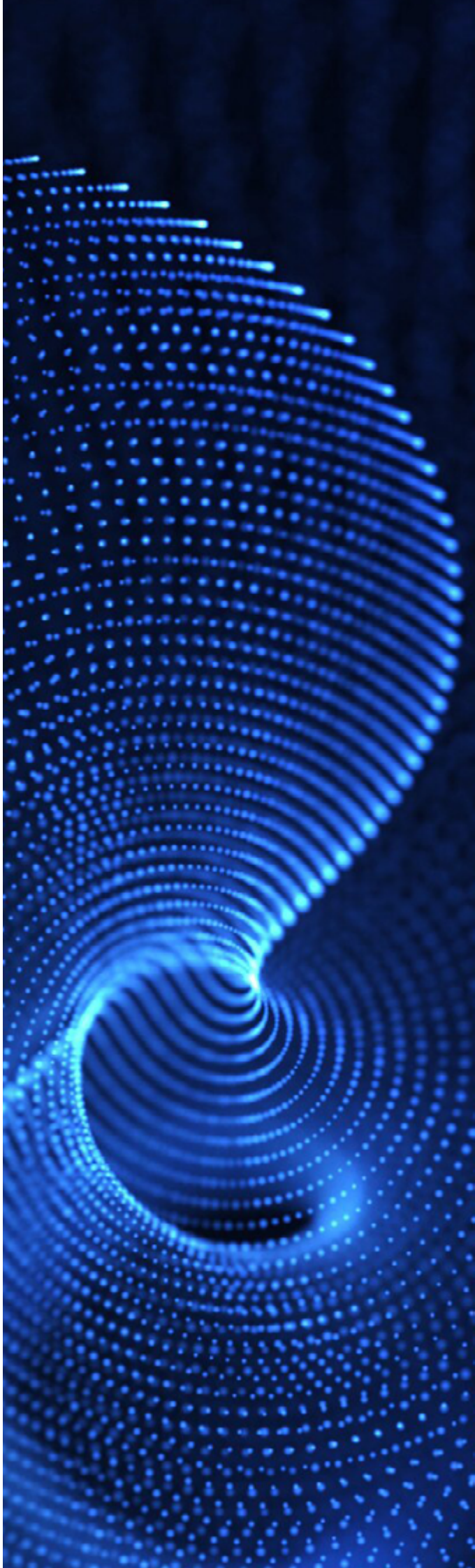
Con el objetivo de afrontar dichas amenazas digitales, que en muchos de los casos traspasan las fronteras de los Estados, se procede a articular los instrumentos adecuados en colaboración e intercambio de la información, y se facilita de esta manera la armonización de la normativa y legislación nacionales, conjuntamente con el desarrollo y mantenimiento de una regulación eficaz y sólida.

En la misma línea, se considera necesario el fomento de la colaboración ciudadana, y llevan a cabo procedimientos de acceso y transmisión de la información de interés público y social.

• Normas globales de ciberseguridad y desafíos geopolíticos

El aumento de la interconexión digital resalta la importancia de establecer normas globales con el fin de garantizar la protección tanto de la infraestructura tecnológica como la seguridad de la información.

No obstante, los intereses estratégicos que poseen los Estados hacen más difícil la implantación de marco normativos y regulatorios globales puesto que requiere su adaptación al régimen jurídico interno.



Áreas de mejora en la normativa vigente

La normativa en materia de ciberseguridad en España y en la UE ha avanzado de forma constante en las últimas décadas. Sin embargo, persisten áreas de mejora para reforzar la protección frente a ciberataques y amenazas emergentes. Estas áreas incluyen aspectos normativos, legales y operativos.

• Sectores no tradicionales en la ciberseguridad

Hasta ahora, la normativa se ha aplicado sobre todo en sectores esenciales como telecomunicaciones, salud, energía o finanzas. Con el avance de la digitalización, otros sectores como la gobernanza, la educación o la agricultura también se exponen a riesgos críticos. Es necesario ampliar el alcance de la regulación para cubrir de manera adecuada estos ámbitos y garantizar una protección integral de la sociedad.

• Protección de la resiliencia de las infraestructuras digitales

Si se parte de que las infraestructuras críticas se establecen como una prioridad, las infraestructuras digitales también deben tener un interés concreto. La Directiva NIS2[54] y la Ley de Ciberresiliencia[55] disponen de referencias en cuanto a las infraestructuras esenciales. Pero no sucede lo mismo en el caso de la protección de las infraestructuras digitales, como pueden ser los centros de procesamiento de datos o las plataformas sobre comunicación digital. Por consiguiente, la normativa vigente aplicable debe reforzar su protección, al hacer especial énfasis en los términos de resiliencia frente a ciberataques coordinados o a gran escala.

• Mejora de la respuesta ante incidentes transnacionales

Los ciberataques de alcance global requieren una coordinación internacional eficaz a través de ENISA y otros organismos competentes. Sin embargo, las diferencias entre los marcos normativos dificultan una respuesta rápida y eficiente. Para superarlo, resulta necesario implantar mecanismos adaptativos que incluyan el intercambio de información sobre amenazas, la gestión conjunta de crisis y la aplicación de procedimientos operativos de mitigación.

• Impulso de la cultura en ciberseguridad

Es preciso reforzar las actividades de sensibilización y los programas de concienciación en colaboración con los sectores público y privado. Se deben coordinar esfuerzos para apoyar a organismos y profesionales en el uso seguro de las tecnologías digitales, promoviendo la adopción de buenas prácticas, estándares y herramientas de seguridad.

• Integración de disposiciones éticas

El desarrollo de tecnologías como la inteligencia artificial o los procesos automatizados plantea nuevos retos en materia de privacidad y protección de datos personales. La normativa debe abordar con mayor claridad la protección ética, para garantizar que las tecnologías emergentes respeten los derechos fundamentales y la libertad digital.

08
Referencias

Estrategias en el ámbito de la Ciberseguridad

• *BOE-A-2015-10389 Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. (s. f.).* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389

• *BOE-A-2019-6347 Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. (s. f.).* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-6347

Normativa específica de Ciberseguridad

• *BOE.es - DOUE-L-2022-81963 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) no 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). (s. f.).* https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

• *Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad a propuesta conjunta de los ministerios del Interior, de Defensa y para la Transformación Digital y de la Función Pública. (s. f.).* https://www.interior.gob.es/opencms/es/detalle/articulo/El-Consejo-de-Ministros-aprueba-el-anteproyecto-de-Ley-de-Coordinacion-y-Gobernanza-de-la-Ciberseguridad/

• *BOE-A-2022-7191 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (s. f.).* https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

• *BOE.es – DOUE-L-2016-1148 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. (s.f.).* https://www.boe.es/doue/2016/194/L00001-00030.pdf

• *BOE-A-2021-1192 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. (s. f.).* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192

Protección de Datos

• *BOE.es - DOUE-L-2016-80807 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). (s. f.).* https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

• *BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (s. f.).* https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

• *BOE.es - DOUE-L-2022-80835 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). (s. f.).* https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-80835

• *BOE.es - DOUE-L-2018-81848 Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) no 1024/2012. (s. f.).* https://www.boe.es/buscar/doc.php?id=DOUE-L-2018-81848

Infraestructuras Críticas

• *BOE.es - DOUE-L-2022-81965 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. (s. f.).* https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81965

• *Regulation - 2022/2554 - EN - DORA - EUR-Lex. (s. f.).* https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

• *BOE-A-2011-7630 Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. (s. f.).* https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

• *BOE-A-2011-8849 Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. (s. f.).* https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849

Seguridad en Productos Digitales y Telecomunicaciones

• *BOE.es - DOUE-L-2024-81720 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) no 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia). (s. f.).* https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81720

• *BOE.es - DOUE-L-2014-81822 Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE. (s. f.).* https://www.boe.es/buscar/doc.php?id=DOUE-L-2014-81822

• *Reglamento - UE - 2024/1183 - EN - EUR-LEX. (s. f.).* https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32024R1183

• *Reglamento - UE - 2019/881 - EN - EUR-LEX. (s. f.).* https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

• *BOE.es - DOUE-L-2018-82056 Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas. (s. f.).* https://www.boe.es/buscar/doc.php?id=DOUE-L-2018-82056

• *BOE.es - DOUE-L-2014-53 Directiva 2014/53/UE del Parlamento Europeo y del Consejo de 16 de abril de 2014 relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE (s. f.).* https://www.boe.es/doue/2014/153/L00062-00106.pdf

• *BOE-A-2010-1331 Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. (s. f.).* https://www.boe.es/buscar/act.php?id=BOE-A-2010-1331

• *BOE-A-2022-4973 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. (s. f.-b).* https://www.boe.es/buscar/doc.php?id=BOE-A-2022-4973

• *BOE-A-2024-8715 Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G. (s. f.).* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2024-8715

Ciberresiliencia

BOE.es - DOUE-L-2025-80049 Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad). (s. f.). https://www.boe.es/buscar/doc.php?id=DOUE-L-2025-80049

Autoridades Competentes en Ciberseguridad

• *Reglamento - 2019/881 - EN - EUR-LEX. (s. f.).* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32019R0881

• *BOE-A-2015-10566 Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. (s. f.).* https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566

• *BOE-A-2024-3791 Real Decreto 205/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa. (s. f.).* https://www.boe.es/buscar/act.php?id=BOE-A-2024-3791

• *BOE-A-2015-10389 Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. (s. f.).* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389

• *BOE-A-2021-9175 Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos. (s. f.).* https://www.boe.es/buscar/act.php?id=BOE-A-2021-9175

• *BOE-A-2002-8628 Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. (s. f.).* https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628

• *BOE.es - DOUE-L-2021-80746 Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación. (s. f.). https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80746*

Gestión de Riesgos en la Ciberseguridad

• *Reglamento de ejecución - UE - 2024/2690 - EN - EUR-Lex. (s. f.).* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L_202402690

• *Reglamento - 2019/881 - EN - EUR-LEX. (s. f.).* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32019R0881

• *Guía Nacional de notificación y gestión de ciberincidentes. (s/f).* Incibe.es https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

• *(s.f.). INCIBE-CERT.* https://www.incibe.es/incibe-cert/incidentes/procedimientos

• *BOE-A-2018-12257 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. (s. f.).* https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257

Notas

[1] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

[2] Orden PJC/522/2025, de 23 de mayo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 24 de abril de 2025, por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia Nacional de Ciberseguridad.

[3] 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 la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148 (*Directiva NIS2*).

[4] Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad a propuesta conjunta de los ministerios del Interior, de Defensa y para la Transformación Digital y de la Función Pública.

[5] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011 (*Reglamento DORA*).

[6] 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 (*Directiva CER*).

[7] 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) nº 526/2013 (*Reglamento sobre la Ciberseguridad*).

[8] 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) nº 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (*Reglamento de Ciberresiliencia*).

[9] CCN-CERT-IA-04-24_Ciberamenazas_y_Tendencias_2024

[10] 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 la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148 (*Directiva NIS2*).

[11] 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 (*Directiva CER*).

[12] Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011 (*Reglamento DORA*).

[13] 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) nº 526/2013 (*Reglamento sobre la Ciberseguridad*).

[14] 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) nº 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (*Reglamento de Ciberresiliencia*).

[15] Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos, y por el que se modifica el Reglamento (UE) 2021/694 (*Reglamento de Cibersolidaridad*).

[16] Orden PJC/522/2025, de 23 de mayo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 24 de abril de 2025, por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia Nacional de Ciberseguridad.

[17] 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) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (*Directiva SRI 2*).

[18] 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*).

[19] 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).

[20] Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

[21] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

[22] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

[23] Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad.

[24] Real Decreto 188/2016, de 6 de mayo, por el que se aprueba el Reglamento por el que se establecen los requisitos para la comercialización, puesta en servicio y uso de equipos radioeléctricos, y se regula el procedimiento para la evaluación de la conformidad, la vigilancia del mercado y el régimen sancionador de los equipos de telecomunicación.

[25] 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).*

[26] Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo de 29 de abril de 2021 por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240.

[27] 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) nº 526/2013.

[28] 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 la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148 (Directiva NIS2).

[29] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

[30] Real Decreto 205/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa.

[31] Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

[32] Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.

[33] Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

[34] Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación.

[35] Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad a propuesta conjunta de los ministerios del Interior, de Defensa y para la Transformación Digital y de la Función Pública.

[36] Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

[37] 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.

[38] *Guía de Gestión de riesgos* de INCIBE.

[39] EEUU, COSO Committee of Sponsoring Organizations of the Treadway Commission.

[40] ISO, International Standarization Association 31000:2009 Risk management – Principles and guideline.

[41] Gobierno de España – Administración Electrónica, Magerit V3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

[42] ISO 27005:2011 Information technology - Security techniques - Information security risk management.

[43] EEUU NIST, National Institute of Standards and Technology.

[44] 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 la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148 (*Directiva NIS2*).

[45] Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza.

[46] 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 la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148 (*Directiva NIS2*).

[47] Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad a propuesta conjunta de los ministerios del Interior, de Defensa y para la Transformación Digital y de la Función Pública.

[48] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y que sustituye, a su vez, al Real Decreto 3/2010.

[49] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

[50] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[51] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

[52] 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.

[53] 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 la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148 (*Directiva NIS2*).

[54] 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 la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148 (Directiva NIS2).

[55] 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) nº 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (*Reglamento de Ciberresiliencia*).

índice de tablas

índice de figuras

glosario

Análisis comparativo de la Normativa y Regulación sobre Ciberseguridad

[I] **Ciberamenaza:** Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización y se sirve de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

[II] **Evaluación de riesgos:** Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

[III] **Sistema de información:** Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

[IV] **Activo de información:** Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

[V] **Vulnerabilidad:** Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del *software* o *hardware* lo solucionará publicando una actualización de seguridad del producto.

[VI] **Integridad:** La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que, de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.

[VII] **Disponibilidad:** Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por personas usuarias o procesos autorizados cuando éstos lo requieran.

[VII] **Confidencialidad:** Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

[IX] **CSIRT:** Acrónimo de *Computer Security Incident Response Team*, también conocido en español como equipo de respuesta a incidentes de seguridad informáticos, es el equipo encargado de recibir, comprobar y responder a incidentes que se detecten en su área de actuación. Es considerado como el equivalente en Europa de su contraparte estadounidense CERT.

[X] **CCN-CERT:** El CCN CERT (Centro Criptológico Nacional Computer Emergency Response Team) es la unidad de respuesta a incidentes de ciberseguridad del Centro Criptológico Nacional, organismo adscrito al Centro Nacional de Inteligencia.

[XI] **ENS:** El Esquema Nacional de Seguridad, de aplicación a todo el Sector Público, así como a los proveedores que colaboran con la Administración, ofrece un marco común de principios básicos, requisitos y medidas de seguridad para una protección adecuada de la información tratada y los servicios prestados, 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.

[xii] **Administración Electrónica:** Actividad consistente en la prestación de servicios a ciudadanía y empresas mediante la utilización de medios telemáticos y definida en la Ley 11/2007 de 22 de junio de acceso electrónico de ciudadanía a los servicios públicos. Esta actividad compete a las Administraciones Públicas con el objeto de simplificar los procedimientos con la Administración, manteniendo al mismo tiempo, los niveles adecuados de seguridad jurídica y procurando la mejora de calidad de los servicios.

[xiii] **Datos personales:** Información relativa a una persona física viva que puede ser identificada o identificable a través de la recopilación de una serie de datos de carácter personal, que establezcan de forma directa o indirecta un perfil más o menos detallado de su identidad personal, familiar o profesional.

[xiv] **CNPIC:** El Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) es un organismo del Ministerio del Interior de España encargado de impulsar, coordinar y supervisar todas las actividades relacionadas con la protección de infraestructuras críticas y la ciberseguridad en el país. Su función es vital para garantizar la seguridad de estas infraestructuras y su trabajo incluye la normativa y la preparación.

[xv] **Cortafuegos:** Sistema de seguridad compuesto o bien de programas (*software*) o de dispositivos *hardware* situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios. La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación. Estos sistemas suelen poseer características de privacidad y autentificación.

[xvi] **Impacto:** Medida del efecto que produce un incidente, desastre, problema o cambio en los niveles de servicio de una empresa y cómo se ven afectados en el caso de que se materialice dicha amenaza.

Las definiciones de los términos de este glosario han sido extraídas de las siguientes fuentes oficiales: Real Academia Española, Gobierno de España, CNI, ENISA, Comisión Europea y Guía de Gestión de Riesgos de INCIBE, salvo alguna excepción que ha sido elaborada por el propio autor del informe.

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es · ontsi · incibe_ · Plan de Recuperación, Transformación y Resiliencia

análisis comparativo de la normativa y regulación sobre ciberseguridad

observaciber