AMENAZAS FÍSICAS Y CIBERNÉTICAS A INFRAESTRUCTURAS Y ENTIDADES CRÍTICAS EN EUROPA

Una visión jurídica a partir del marco normativo actualmente vigente en la Unión Europea y su grado de transposición en Alemania y España

MIGUEL ÁNGEL CANO PAÑOS[1]
macano@ugr.es

Cómo citar/Citation
Cano Paños, Miguel Ángel (2026).
Amenazas físicas y cibernéticas a infraestructuras y entidades críticas en Europa.
Una visión jurídica a partir del marco normativo actualmente vigente en
la Unión Europea y su grado de transposición en Alemania y España.
Revista de Derecho Comunitario Europeo, 83, 83-126.
doi: https://doi.org/10.18042/cepc/rdce.83.03

Resumen

Teniendo en cuenta el escenario actual del que es testigo la propia Unión Europea (UE), con el conflicto bélico entre Rusia y Ucrania que se desarrolla muy cerca de las fronteras de la Unión, y con la sombra de la amenaza que se cierne sobre determinados países europeos, así como considerando distintos incidentes que han afectado a sectores como la energía y el transporte a nivel comunitario, la protección de aquellas infraestructuras críticas que proporcionan bienes y servicios esenciales para la

[1] Catedrático de Derecho Penal y Criminología. Universidad de Granada. Este trabajo es fruto de dos estancias de investigación realizadas por el autor. La primera de ellas en agosto de 2024 en la Universidad de Münster (Alemania); la segunda en agosto del año 2025 en la Universidad de Navarra. El trabajo se inscribe dentro del Proyecto de Investigación «Análisis cuantitativo y fenomenológico de las amenazas cibernéticas a infraestructuras críticas nucleares y su impacto en la protección radiológica (CIBERCLEAR)», financiado por el Consejo de Seguridad Nuclear, cuyo investigador principal es el Prof. Dr. Miguel Olmedo Cardenete. Referencia del Proyecto: PRY015/23.

población adquiere una importancia trascendental. Partiendo del contexto descrito, el presente trabajo tiene como objetivo realizar una aproximación jurídica tanto al marco legislativo aprobado en las últimas fechas sobre dicha materia por la UE como a su grado de transposición al ordenamiento de los Estados miembros. Para ello, en dicho análisis se prestará especial atención a los casos de Alemania y España, desde un enfoque jurídico comparado. Mientras que en el primero de ellos, el actual Gobierno ha logrado recientemente transponer a su ordenamiento interno las directivas comunitarias aprobadas en el año 2022 para la protección física y cibernética de las infraestructuras y entidades críticas, en el caso de España existen únicamente hasta el momento sendos anteproyectos de ley, por lo que dicha transposición de la normativa comunitaria está todavía lejos de producirse.

Palabras clave

Infraestructuras críticas; entidades críticas; amenazas cibernéticas; resiliencia; directivas Unión Europea; Alemania; España; derecho comparado.

PHYSICAL AND CYBER THREATS TO CRITICAL INFRASTRUCTURE AND ENTITIES IN EUROPE

A legal perspective based on the regulatory framework currently in force in the European Union and its degree of transposition in Germany and Spain

Abstract

Taking into account the current scenario that the European Union (EU) itself is witnessing, with the war conflict between Russia and Ukraine taking place very close to the borders of the Union, and with the shadow of the threat looming over certain European countries, as well as considering different incidents that have affected sectors such as energy and transport at the community level, the protection of those critical infrastructures that provide essential goods and services to the population acquires transcendental importance. Based on the described context, this paper aims to provide a legal overview of both the legislative framework recently approved by the EU on this matter and its degree of transposition into the legal systems of the Member States. To this end, the analysis will pay special attention to the cases of Germany and Spain, from a comparative legal perspective. While in the first case, the current Government has recently managed to transpose into its internal regulations the Community directives approved in 2022 for the physical and cyber protection of critical infrastructures and entities, in the case of Spain there are only two draft bills so far, so the transposition of Community regulations is still far from happening.

Keywords

Critical infrastructures; critical entities; cyber threats; resilience; European Union directives; Germany; Spain; comparative law.

MENACES PHYSIQUES ET CYBERNÉTIQUES PESANT SUR LES INFRASTRUCTURES ET LES ENTITÉS CRITIQUES EN EUROPE

Une approche juridique fondée sur le cadre réglementaire actuellement en vigueur dans l'Union européenne et son degré de transposition en Allemagne et en Espagne

Résumé

Compte tenu du contexte actuel auquel est confrontée l'Union européenne (UE), avec le conflit armé entre la Russie et l'Ukraine qui se déroule tout près des frontières de l'Union, et avec l'ombre de la menace qui pèse sur certains pays européens, ainsi que des différents incidents qui ont touché des secteurs tels que l'énergie et les transports au niveau communautaire, la protection des infrastructures critiques qui fournissent des biens et des services essentiels à la population revêt une importance capitale. Dans ce contexte, le présent document vise à analyser juridiquement la législation européenne récemment adoptée en la matière et son degré de transposition dans les systèmes juridiques des États membres. À cette fin, cette analyse accordera une attention particulière aux cas de l'Allemagne et de l'Espagne, dans une perspective juridique comparative. Alors que dans le premier cas, le gouvernement actuel a récemment réussi à transposer dans son ordre juridique interne les directives communautaires adoptées en 2022 pour la protection physique et cybernétique des infrastructures et des entités critiques, dans le cas de l'Espagne, il n'existe pour l'instant que des avant-projets de loi, de sorte que cette transposition de la réglementation communautaire est encore loin d'être réalisée.

Mots-clés

Infrastructures critiques; entités critiques; cybermenaces; résilience; directives de l'Union européenne; Allemagne; Espagne; droit comparé.

SUMARIO

I. INTRODUCCIÓN

Las infraestructuras y entidades críticas constituyen sin lugar a dudas no solo un elemento central a la hora de prestar bienes y servicios considerados como esenciales para la población, sino también un sector muy importante en la configuración de la seguridad nacional. Sus operadores deben estar continuamente preparados contra peligros tales como desastres naturales, errores humanos, obsolescencia de las instalaciones, actos de sabotaje, ciberataques y, en última instancia, terrorismo. Para poder reaccionar con flexibilidad a las diferentes amenazas, la resiliencia constituye un elemento clave[2]. Esta resiliencia debe aplicarse no solo a las amenazas físicas o procedentes de entornos *offline,* sino también a las conocidas como ciberamenazas.

El grado de amenaza al que se pueden ver expuestas las infraestructuras críticas (IC), ya sea aquella provocada por el hombre, o bien por incidentes o desastres naturales, pudo comprobarse en España el pasado día 28 de abril de 2025, cuando, como consecuencia de un apagón, se produjo una interrupción

[2] La resiliencia hace referencia a la capacidad de un sistema para resistir o adaptarse a los eventos, manteniendo o recuperando rápidamente su funcionalidad.

generalizada del suministro eléctrico durante más de doce horas, afectando principalmente a la España peninsular, Portugal continental, Andorra, así como, en menor grado, a zonas del sur de Francia. Dicho corte de energía provocó importantes dificultades no solo en las telecomunicaciones y el sistema de transporte, sino que además afectó a todos aquellos sectores dependientes en mayor o menor medida de Internet, el cual se cayó durante la mayor parte del día. El informe presentado el pasado 17 de junio de 2025 por el Ministerio de Transición Ecológica y el Reto Demográfico concluyó que el apagón tuvo una causa multifactorial derivada de una combinación de fallos técnicos como oscilaciones de frecuencia mal amortiguadas, una programación deficiente del sistema eléctrico y respuestas incorrectas de algunas plantas generadoras, descartándose por completo un ciberataque[3]. En paralelo, en el citado informe se identificaban una serie de vulnerabilidades en la infraestructura digital que debían ser corregidas para con ello aumentar la ciberseguridad del sistema eléctrico.

Por lo que hace referencia a Alemania, debe destacarse el apagón que el pasado 4 de enero del presente año 2026 afectó a una amplia zona del suroeste de Berlín, y que dejó sin luz durante varios días a más de 30 000 hogares. Dicho apagón tuvo su origen en un incendio en una instalación eléctrica provocado por un grupo anarquista denominado Vulkangruppe. La Fiscalía alemana inició las pertinentes investigaciones de cara a encontrar a los presuntos culpables, al considerar que el acto de sabotaje constituyó un acto de terrorismo vinculado a la extrema izquierda[4].

A nivel europeo conviene hacer referencia al último incidente que ha afectado a IC del sector del transporte, como son los aeropuertos. Así, el pasado 19 de septiembre de 2025 se produjo un ciberataque masivo que afectó principalmente a los aeropuertos de Bruselas, Berlín, Londres y Dublín, prolongándose durante todo ese fin de semana. El objetivo del ataque era en concreto la empresa Collins Aerospace, un proveedor externo de servicios de procesa-

[3] Véase: «El Gobierno presenta el informe sobre las causas del apagón, que se debió a una sobretensión de origen "multifactorial"», *La Moncloa,* 17 de junio de 2025. Disponible en: https://bit.ly/3ORTttk. Al parecer, como consecuencia de la creciente integración de energías renovables intermitentes, como la solar y la eólica, el día 28 de abril de 2025 la energía solar estaba generando casi el 60 % de la electricidad, produciéndose un grave desequilibrio entre la producción de electricidad y la demanda de la misma en ese concreto día, lo que generó un denominado «hueco de tensión» que terminó de llevar el suministro al colapso.

[4] Véase: «Berlín a oscuras: 30 500 hogares siguen sin luz tras el presunto sabotaje de un grupo de extrema izquierda», *El Mundo,* edición de 5 de enero de 2026. Disponible en: https://is.gd/uUWmXn.

miento de datos, encargado de gestionar los sistemas electrónicos de facturación y embarque para distintas aerolíneas. Como consecuencia del ciberataque se registraron retrasos y cancelaciones de centenares de vuelos, con consecuencias directas para miles de pasajeros y pérdidas millonarias en el sector aéreo. A raíz de este último incidente, expertos en ciberseguridad aérea han vuelto a hacer hincapié en la necesidad de que los aeropuertos inviertan más en resiliencia digital, planes de contingencia y pruebas de estrés que les permitan seguir funcionando incluso si un proveedor externo falla. Paralelamente, la Comisión Europea ha instado a los Estados miembros a transponer y aplicar plenamente la nueva directiva sobre redes y los sistemas de información (conocida como NIS-2, a la que se hará referencia explícita *infra*), para con ello evitar amenazas e incidentes cibernéticos como este último ataque al *software* de facturación y embarque de varios aeropuertos comunitarios[5].

Para fortalecer la resiliencia de las IC frente a las ciberamenazas y aquellas otras procedentes de entornos físicos o naturales, la Unión Europea (UE) ha adoptado en las últimas fechas una serie de resoluciones de importancia, las cuales resultan de obligado cumplimiento para los Estados miembros. A destacar es, sobre todo, la Estrategia de Ciberseguridad de la Unión Europa para la Década Digital, aprobada el 14 de diciembre de 2020 (Comisión Europea, 2020), en la cual se avanzaban una serie de propuestas elaboradas por la Comisión que finalmente fructificaron en dos directivas aprobadas ambas en el año 2022; una de ellas dirigida a impulsar una serie de medidas destinadas a garantizar un elevado nivel de ciberseguridad en toda la Unión en lo relativo a las infraestructuras críticas[6] y una segunda cuyo objetivo es aumentar la resiliencia física de las denominadas entidades críticas[7]. En ambas directivas se señalaba de forma taxativa que los países miembros de la UE

5 «Un detenido en Inglaterra por el supuesto ciberataque que afectó a aeropuertos europeos», *EuroEFE,* edición de 24 de septiembre de 2025. Disponible en: https://is.gd/LhsyiR.

6 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 (*DOUE* núm. 333, de 27 de diciembre de 2022, pp. 80-152) (Directiva NIS-2).

7 Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas (*DOUE* núm. 333, de 27 de diciembre de 2022, pp. 164-198) (Directiva CER). A efectos meramente aclaratorios, el concepto de *entidad crítica* resulta más amplio que el de *infraestructura crítica,* ya que esta última constituye en esencia una instalación concreta de una entidad. Por tanto, puede afirmarse que una infraestructura crítica está vinculada a una entidad crítica, de la que forma parte.

debían llevar a cabo su transposición a sus ordenamientos jurídicos nacionales a más tardar el 17 de octubre de 2024. Sin embargo, son numerosos los países que todavía no han llevado a cabo dicha transposición, entre ellos España.

A partir de lo señalado en los párrafos anteriores, el objetivo del presente artículo, el cual viene a constituir la segunda de las dos partes de la investigación que se encuentra en la base del mismo[8], es analizar, desde una perspectiva eminentemente jurídica, el marco legal actualmente vigente en Europa en el contexto de la protección de las infraestructuras y entidades críticas; no solo en el contexto del derecho comunitario europeo, sino también en determinados países de la UE, en concreto Alemania y España. Al contrario de lo sucedido en España, en Alemania se elaboraron durante el año 2024 sendos proyectos de ley dirigidos a transponer al ordenamiento jurídico germano las dos directivas a las que se ha hecho alusión en el párrafo anterior; proyectos de ley que, en el momento de concluir el presente trabajo, han fructificado en dos leyes aprobadas en las últimas semanas que han permitido transponer al ordenamiento germano las mencionadas directivas aprobadas en el año 2022. En el polo opuesto, España cuenta únicamente con sendos anteproyectos, aprobados respectivamente en enero y mayo del año 2025, los cuales tienen como objetivo la efectiva transposición de las directivas 2022/2555 y 2022/2557.

Para ello, y tras la presente introducción, el trabajo se ocupa de analizar el marco actualmente vigente en la UE con el objetivo de proteger a las infraestructuras y entidades críticas frente a amenazas (epígrafe II). A continuación, el epígrafe III se enfoca en las medidas adoptadas en Alemania para combatir las amenazas (*offline* y *online*) a sus estructuras y entidades críticas. Así, y tras exponer la configuración teórica y organizativa que en Alemania se hace de las IC (III.1.), el trabajo se detiene a presentar los inicios legislativos impulsados para proteger a las mismas, los cuales, como se verá, se enfocaron fundamentalmente en la protección frente a ciberamenazas (III.2.). Seguidamente, el trabajo se centra en presentar los proyectos de ley elaborados en el año 2024 en Alemania con el objetivo de incorporar al ordenamiento jurídico germano la legislación aprobada en el seno de la UE (III.3). Por último, y antes de entrar en las conclusiones, el trabajo dirige su mirada al contexto español, presentando las medidas legislativas que hasta la fecha se han aprobado para incorporar al ordenamiento jurídico español las directivas a las que se ha hecho referencia *supra* (epígrafe IV).

[8] La primera parte, de marcado carácter criminológico, se ocupó de analizar las amenazas que se ciernen sobre las infraestructuras críticas a nivel europeo, haciendo especial referencia a las centrales nucleares. Véase Cano Paños (2025).

Desde un punto de vista metodológico, la decisión de utilizar en este trabajo un enfoque jurídico comparado responde a la idea de indagar en el grado de transposición de las directivas 2022/2555 y 2022/2557 en los Estados miembros de la UE, ya que, como se ha señalado *supra,* ambas directivas deberían haber sido incorporadas al ordenamiento jurídico interno a más tardar el pasado 17 de octubre de 2024. El hecho de centrarse en el caso de Alemania se debe a una estancia de investigación realizada en dicho país por el autor del presente trabajo durante el mes de agosto del año 2024. Ello permitió tener acceso directo a todos los materiales legislativos elaborados por el anterior Gobierno germano de cara a la implementación de las mencionadas directivas, lo cual se convirtió en un objetivo prioritario debido a diferentes incidentes provocados que afectaron a infraestructuras y entidades críticas situadas en Alemania o relacionadas con ella.

II. LA ESTRATEGIA DE CIBERSEGURIDAD DE LA UNIÓN EUROPEA PARA LA DÉCADA DIGITAL, DE 14 DE DICIEMBRE DE 2020, Y SUS REPERCUSIONES PARA LOS ESTADOS MIEMBROS

1. INTRODUCCIÓN. ASPECTOS RELEVANTES DE LA ESTRATEGIA Y SUS CONSECUENCIAS

Teniendo en cuenta el nivel de amenazas a las que se pueden ver expuestas las IC que actúan en los Estados miembros de la UE, el legislador europeo se ha venido poniendo como objetivo ampliar la normativa sobre la protección física y cibernética de las IC. En el marco de dicha legislación conviene sobre todo destacar la Estrategia de Ciberseguridad de la UE, adoptada el 14 de diciembre de 2020 (Comisión Europea, 2020).

Aunque no va a ser objeto de análisis en el presente trabajo, conviene aquí hacer mención del Reglamento (UE) 2022/2554[9], también conocido como Reglamento DORA (Digital Operational Resilience Act). Dicho reglamento, el cual entró en vigor el 16 de enero de 2023 y comenzó a aplicarse a partir del 17 de enero de 2025, tiene como objetivo reforzar la seguridad informática de entidades financieras como bancos, compañías de seguros y

[9] 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) núm. 1060/2009, (UE) núm. 648/2012, (UE) núm. 600/2014, (UE) núm. 909/2014 y (UE) 2016/1111 (DO L 333, de 27 de diciembre de 2022).

empresas de inversión, y garantizar que el sector financiero, dentro del ámbito de la UE, pueda mantener un elevado nivel de resiliencia en caso de perturbaciones operativas graves fruto, por ejemplo, de ciberataques o incidentes. Dicho reglamento armoniza las normas relativas a la resiliencia operativa del sector financiero aplicables a veinte tipos diferentes de entidades financieras, así como de proveedores terceros de servicios de tecnologías de la información y comunicación (TIC). Efectivamente, tal y como se ha señalado, el Reglamento DORA supone un cambio de paradigma para la regulación de la ciberseguridad de las entidades financieras, ya que, por primera vez, los prestadores de servicios tecnológicos (proveedores de servicios TIC) entran dentro de su ámbito subjetivo de aplicación (Gómez Castro y Montilla Castilla, 2025; González García, 2025). Hasta ahora, estos proveedores estaban obligados a cumplir con ciertas obligaciones de seguridad en sus relaciones con las entidades financieras, en la medida en que los contratos con estas entidades debían tener un contenido obligatorio en materia de ciberseguridad. Sin embargo, la aplicación del Reglamento DORA supone que ciertas obligaciones sean de aplicación directa a estos proveedores, sin depender únicamente del concreto contrato suscrito.

La arriba mencionada Estrategia del año 2020 tiene como primer objetivo fortalecer la resiliencia ante las ciberamenazas y garantizar que tanto los ciudadanos como las empresas puedan beneficiarse de tecnologías digitales dignas de confianza. Por ello, el legislador europeo pretende promover normas encaminadas a soluciones de calidad, así como estándares de ciberseguridad para aquellos bienes y servicios esenciales vinculados a las IC, impulsando el desarrollo y la aplicación de nuevas tecnologías bajo unos márgenes de seguridad que impidan amenazas procedentes del ciberespacio.

Siguiendo los avances logrados en las estrategias anteriores, la Estrategia aprobada en el año 2020 contiene propuestas concretas para la aplicación de tres instrumentos principales. Estos tres instrumentos son: iniciativas de regulación, de inversión y políticas. Las mismas deben centrarse en tres áreas de acción de la UE:

1. Resiliencia, soberanía tecnológica y liderazgo.
2. Capacidad operativa para impedir, disuadir y responder.
3. Cooperación para promover un ciberespacio global y abierto.

Con todo, la Estrategia del año 2020 no se centra exclusivamente en la ciberresiliencia de IC, sino que también tiene en cuenta la resiliencia física. A partir de estas consideraciones, dicha estrategia contempla dos propuestas legislativas, las cuales se ocupan respectivamente de la resiliencia cibernética y física de las IC y las redes: Directiva NIS-2 y Directiva CER, que cubren una

amplia gama de sectores y tienen como objetivo abordar los riesgos actuales y futuros —ya sean estos *online* u *offline* (desde ciberataques hasta desastres naturales)— de una manera coherente y complementaria.

Tal y como señala la Estrategia del año 2020, los riesgos de ciberseguridad siguen evolucionando con el aumento de la digitalización y la interconexión. Los riesgos físicos también son cada vez más complejos desde la adopción, en 2008, de las normas de la UE sobre infraestructuras críticas, que en el año 2020 se aplicaban exclusivamente a los sectores de la energía y el transporte[10]. Por ello, el objetivo de las revisiones que se llevan a cabo por ambas directivas, aprobadas en el año 2022, es actualizar las normas según la lógica de la Estrategia de la UE para una Unión de la Seguridad, superar la falsa dicotomía entre lo que está en línea y fuera de ella, así como romper con el enfoque compartimentado.

2. LA DIRECTIVA NIS-2

La primera directiva a la que hace alusión la Estrategia de la UE del año 2020 está dirigida de forma exclusiva a la protección de las IC frente a amenazas procedentes del ciberespacio[11]. En concreto, el objetivo de la Directiva NIS-2[12] es introducir medidas vinculantes para la administración y la economía con las cuales se debe garantizar un elevado nivel común de ciberseguridad en toda la UE. Con ello se pretende proteger a entidades importantes y especialmente importantes de los daños causados por ciberataques, mejorando al mismo tiempo el funcionamiento del mercado interior europeo.

En la misma se señala que las diferencias existentes entre los Estados miembros a la hora de definir y proteger IC frente a ciberamenazas no solo conllevan una fragmentación del mercado interior; en última instancia, esas diferencias pueden derivar también en una mayor vulnerabilidad de algunos Estados miembros, cuyos efectos pueden llegar a sentirse en toda la UE. Por consiguiente, el objetivo de la Directiva 2022/2555 es eliminar esas divergencias tan pronunciadas entre los Estados miembros, obligando a estos a definir una estrategia nacional de ciberseguridad para hacer frente a las amenazas. En concreto, la mencionada directiva hace referencia a la definición

[10] 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 (DO L 345, de 23 de diciembre de 2008, pp. 75-82).

[11] Sobre esta Directiva NIS-2, véanse los trabajos de Barrio Andrés (2024) y Canós Guillamón (2025).

[12] NIS es el acrónimo de Network and Information Systems.

de normas mínimas relativas al funcionamiento de un marco regulador coordinado, el establecimiento de mecanismos para que las autoridades competentes de cada Estado miembro cooperen de manera eficaz, la actualización de la lista de sectores y actividades sujetos a las obligaciones de ciberseguridad y la disponibilidad de vías de recurso y medidas de ejecución eficaces, que son fundamentales para garantizar el cumplimiento efectivo de dichas obligaciones.

Ahora bien, teniendo en cuenta las interrelaciones que existen entre la ciberseguridad y la seguridad física de las entidades consideradas como críticas, la propia Directiva 2022/2555 señala expresamente que debe garantizarse un enfoque coherente e integrador entre dicha directiva y la Directiva (UE) 2022/2557, relativa a la resiliencia física de las entidades críticas. Para ello, cada Estado miembro debe velar por que sus estrategias nacionales de ciberseguridad establezcan un marco de actuación para mejorar la coordinación dentro de dicho Estado miembro entre las autoridades competentes con arreglo a la Directiva 2022/2555 y las competentes con arreglo a la Directiva 2022/2557, en el contexto del intercambio de información sobre los riesgos, ciberamenazas e incidentes relacionados con la ciberseguridad, así como sobre los riesgos, amenazas e incidentes no relacionados con la ciberseguridad, y sobre el ejercicio de las tareas de supervisión. Además, las autoridades competentes con arreglo a la Directiva 2022/2555 y las que lo son en relación a la Directiva 2022/2557 deben cooperar e intercambiar información sin demora indebida, en particular en lo que hace referencia a la identificación de las entidades críticas, los riesgos, las ciberamenazas e incidentes relacionados con la ciberseguridad, así como en lo que respecta a los riesgos, amenazas e incidentes no relacionados con la ciberseguridad que afecten a las entidades críticas, incluidas las medidas de ciberseguridad y físicas adoptadas por las entidades críticas, así como en lo que se refiere a los resultados de las actividades de supervisión realizadas con respecto a dichas entidades.

3. LA DIRECTIVA CER

Frente al contenido regulador de la Directiva 2022/2555, la Directiva CER[13] que aquí se analiza se centra en la protección física de las denominadas «entidades críticas» en el seno de la UE[14]. Dicha directiva sustituye a la Directiva Europea de Infraestructuras Críticas del año 2008, introduciendo

[13] CER constituye el acrónimo de Critical Entities Resilience.

[14] Sobre la Directiva CER pueden, entre otros, consultarse los siguientes trabajos: Álvarez Fernández (2023) y KPMG (2025).

nuevas reglas para fortalecer la resiliencia de las entidades críticas ante una serie de amenazas, incluidos peligros naturales, ataques terroristas, amenazas internas o sabotaje.

Con la Directiva 2022/2557 se ha creado un marco jurídico europeo uniforme para fortalecer la resiliencia de las entidades críticas en al menos once sectores frente a amenazas, más allá de la protección de la seguridad informática en el mercado interior[15]. El objetivo de la Directiva es establecer obligaciones mínimas uniformes para las entidades críticas y garantizar su implementación mediante medidas de apoyo y supervisión coherentes y específicas. Para fortalecer la resiliencia de estas entidades críticas, las cuales resultan cruciales para el buen funcionamiento del mercado interior, la Directiva 2022/2557 crea un marco general («paraguas»), el cual, en el sentido de un enfoque de todos los peligros, tiene en cuenta los peligros naturales o los peligros provocados por el hombre, ya sean accidentales o intencionados.

En la misma se señala que las entidades que explotan las infraestructuras consideradas como críticas han de estar mejor equipadas para hacer frente a los riesgos para sus operaciones que puedan dar lugar a una perturbación en la prestación de servicios esenciales. Al respecto, afirma que actualmente existe un panorama dinámico de amenazas, entre las que figuran las amenazas híbridas y terroristas en evolución, así como las crecientes interdependencias entre infraestructura y sectores. Además, ha aumentado el riesgo físico derivado de las catástrofes naturales y del cambio climático, que intensifica la frecuencia y la magnitud de los fenómenos meteorológicos extremos e introduce cambios a largo plazo en las condiciones climáticas medias que pueden mermar la capacidad, la eficiencia y la vida útil de determinados tipos de infraestructuras y entidades en caso de no existir medidas de adaptación al cambio climático. Como se puede observar, el foco de atención de esta directiva se centra en la protección física de las entidades críticas, al no hacerse alusión alguna a las ciberamenazas, objeto como se sabe de la Directiva 2022/2555. De este modo, la Directiva 2022/2557 crea un marco general que aborda la resiliencia de las entidades críticas con respecto a todos los peligros, ya sean naturales o provocados, accidental o intencionadamente, por el ser humano.

[15] Estos sectores son los siguientes: energía, transporte, banca, infraestructuras de mercados financieros, salud, agua potable, aguas residuales, infraestructura digital, administración pública, espacio y alimentación. En virtud de ella, los Estados miembros deberán adoptar una estrategia nacional y llevar a cabo evaluaciones periódicas de riesgos para identificar las entidades que se consideran críticas o vitales para la sociedad y la economía.

Por otro lado, la Directiva 2022/2557 afirma que el mercado interior se caracteriza por la fragmentación en lo que respecta a la identificación de las entidades críticas, pues los sectores y categorías de entidades pertinentes no se reconocen sistemáticamente como críticos en todos los Estados miembros. Por consiguiente, la Directiva que aquí se analiza tiene como uno de sus objetivos lograr un nivel sustancial de armonización en lo que se refiere a los sectores y categorías de entidades que entran en su ámbito de aplicación.

Y es que las entidades que intervienen en la prestación de servicios esenciales están cada vez más sujetas a requisitos divergentes impuestos por el derecho nacional. El hecho de que algunos Estados miembros tengan unos requisitos menos estrictos para esas entidades críticas no solo conduce a distintos niveles de resiliencia, sino que también acarrea una carga administrativa adicional e innecesaria para las empresas que realizan operaciones transfronterizas, en particular en el caso de aquellas que tienen actividad en Estados miembros con unos requisitos más estrictos. Por consiguiente, un marco de la Unión uniforme también debe conducir a condiciones de competencia equitativas para las entidades críticas en toda la UE.

Con el fin de garantizar un enfoque global de la resiliencia de las entidades críticas, cada Estado miembro debe contar con una estrategia que mejore la resiliencia de las entidades críticas. Dicha estrategia debe establecer los objetivos estratégicos y las medidas de actuación que hayan de aplicarse. A fin de alcanzar ese enfoque global, los Estados miembros deben garantizar que sus estrategias establezcan un marco de actuación para mejorar la coordinación entre las autoridades competentes con arreglo a la Directiva 2022/2557 y las autoridades competentes con arreglo a la Directiva 2022/2555, en el contexto del intercambio de información sobre los riesgos, amenazas e incidentes relacionados con la ciberseguridad y los riesgos, amenazas e incidentes no relacionados con ella y en el contexto del ejercicio de las tareas de supervisión. Como se sabe, a dicha interdependencia y coordinación entre la protección física y cibernética hace también alusión la Directiva 2022/2555, analizada en el epígrafe anterior.

Por otro lado, cada Estado miembro debe realizar, en un marco armonizado, una evaluación de los riegos naturales y de origen humano pertinentes, incluidos los de carácter transfronterizo o intersectorial, que puedan afectar a la prestación de servicios esenciales, incluidos los accidentes, las catástrofes naturales, las emergencias de salud pública como las pandemias y las amenazas híbridas u otras amenazas antagónicas, incluidos los delitos de terrorismo, la infiltración delictiva y el sabotaje.

Por último, en la Directiva 2022/2557 se señala que los Estados miembros deben designar o establecer autoridades competentes para supervisar la aplicación y, en su caso, hacer cumplir las normas de la mencionada directiva,

y garantizar que dichas autoridades dispongan de las competencias y los recursos adecuados.

Tanto la Directiva 2022/2555 como la Directiva 2022/2557 establecían que los Estados miembros debían transponerlas al derecho nacional en el plazo de veintiún meses a partir de su entrada en vigor. Teniendo en cuenta que ambas directivas entraron en vigor el 16 de enero de 2023 (es decir, veinte días después de su publicación en el *DOUE*), los Estados miembros debían adoptar y publicar las medidas necesarias para dar cumplimiento a lo establecido en ambas directivas antes del 17 de octubre del año 2024. Como se verá en los epígrafes siguientes, en el caso de Alemania, ya durante el año 2024 se elaboraron proyectos de ley consolidados dirigidos a transponer al ordenamiento jurídico germano el contenido de ambas directivas. En el momento de concluir el presente trabajo, dichos proyectos han desembocado finalmente en la aprobación de sendas leyes mediante las cuales se ha logrado transponer al ordenamiento jurídico germano las directivas del año 2022. En el polo opuesto, en España solo existen en estos momentos sendos anteproyectos de ley con el punto de mira puesto respectivamente en la Directiva 2022/2555, así como en la Directiva 2022/2557, por lo que en este último país la transposición de la normativa europea con respecto a la protección física y cibernética de entidades e infraestructuras críticas se encuentra todavía muy lejos en el horizonte.

III. APROXIMACIÓN JURÍDICA A LAS MEDIDAS LEGISLATIVAS ADOPTADAS EN ALEMANIA PARA COMBATIR LAS AMENAZAS A INFRAESTRUCTURAS Y ENTIDADES CRÍTICAS

1. PREÁMBULO. DEFINICIÓN DE CONCEPTOS (KRITIS). PROTECCIÓN ANALÓGICA Y DIGITAL DE LAS INFRAESTRUCTURAS CRÍTICAS EN ALEMANIA

Lo primero que resulta necesario al comienzo de este epígrafe es saber qué se entiende en Alemania por infraestructuras críticas (IC). Al respecto, en el país germano se suele utilizar a menudo el término KRITIS, aunque también, en no pocas ocasiones, se puede encontrar el concepto de infraestructuras críticas *(kritische Infrastrukturen)*.

Según una definición acuñada por el Gobierno federal: «Las infraestructuras críticas (KRITIS) son organizaciones o instalaciones de gran importancia para la comunidad estatal, cuya caída o deterioro daría lugar a cuellos de botella duraderos en el suministro, perturbaciones importantes en la seguridad pública u otras consecuencias dramáticas» (Bundesamt für Sicherheit in der

Informationstechnik, s. f.). Por estas razones, garantizar la protección de estas infraestructuras constituye una tarea fundamental para el Estado y la economía, así como un tema central de la política y seguridad alemanas.

Conviene señalar que el acrónimo KRITIS y la expresión *kritische Infrastrukturen* a veces se utilizan como sinónimos, si bien, en ocasiones, KRITIS se refiere a un espectro más amplio de infraestructuras que las previstas en la Ley de la Oficina Federal de Seguridad de la Información (BSI-Gesetz), la cual aquí únicamente se apunta, ya que será analizada en el epígrafe siguiente.

Las IC son infraestructuras que resultan particularmente importantes para el funcionamiento de la comunidad y para asegurar las necesidades básicas de la población. Las mismas se caracterizan por que, en caso de interrupciones o fallos, se perjudicarían significativamente procesos esenciales de la vida diaria de una gran parte de la población. Por tanto, la protección de las IC en Alemania reviste gran importancia económica y social (Beucher *et al.,* 2023: 502). En lo que respecta a este concreto país, los operadores de aquellas instalaciones pertenecientes a una infraestructura crítica son los principales responsables de protegerlas. Estos deben estar completamente preparados contra peligros tales como desastres naturales, terrorismo, sabotaje y también errores humanos. Para poder reaccionar con flexibilidad a las diferentes amenazas, la resiliencia de las IC adquiere cada vez mayor importancia.

El actual Ministerio Federal del Interior (BMI, por sus siglas en alemán)[16] es responsable, dentro del Gobierno federal, de coordinar las actividades, estrategias y medidas para la mejor protección posible de las IC (Bundesministerium des Innern und für Heimat, s. f.). Para ello, en octubre del año 2022 se puso en marcha un Centro Conjunto de Coordinación de Infraestructuras Críticas (Gemeinsamer Koordinierungsstab Kritischer Infrastruktur, GEKKIS, por sus siglas en alemán) (Bundesministerium des Innern und für Heimat, 2022). Este organismo tiene, entre otras, las siguientes funciones:

[16] Tras el triunfo de la Unión Cristiano-Demócrata (CDU, por sus siglas en alemán) en las elecciones legislativas celebradas el pasado mes de febrero de 2025 en Alemania, se ha formado un nuevo Gobierno integrado por una denominada «gran coalición» entre la CDU y el Partido Socialdemócrata (SPD). Con ello, el Ministerio del Interior germano ha recuperado su anterior nomenclatura (Bundesministerium des Innern). Con el anterior Gobierno liderado por el SPD, dicho ministerio se denominaba Bundesministerium des Innern und für Heimat (Ministerio del Interior y de la Patria). Por ello, en el presente trabajo se utilizará una u otra variante a la hora de denominar a dicho ministerio en función del partido político que lideraba en cada momento la coalición de gobierno.

1. Proporcionar los informes de situación más actualizados para la protección de IC. De este modo, todos los sectores implicados tienen una visión general de la situación de riesgo actual.
2. Permitir un intercambio estructurado entre los sectores para identificar desafíos comunes y trabajar juntos para superarlos.
3. Reunirse inmediatamente como grupo *ad hoc* en caso de incidentes relevantes. La infraestructura de emergencia existente en el Centro de Situación (*Lagezentrum*) del actual Ministerio del Interior garantiza la accesibilidad las veinticuatro horas del día, los siete días de la semana, a los encargados de la toma de decisiones en los ministerios relevantes (Bundesministerium des Innern und für Heimat, 2022).

Tal y como se ha señalado ya anteriormente, las IC, por ejemplo, en los sectores de la salud, la energía o los transportes, resultan indispensables para suministrar a los ciudadanos bienes y servicios vitales. La mayoría de estas IC dependen actualmente en gran medida de la tecnología de la información (TI). Este desarrollo seguirá aumentando en el futuro en el contexto de la creciente digitalización de la economía, el Estado y la sociedad. La digitalización crea, sin duda, nuevas oportunidades. Sin embargo, esta dependencia también hace que la sociedad sea vulnerable. Dado que una gran parte de las IC en Alemania se encuentra en manos privadas, su protección contra las amenazas procedentes del ciberespacio solo puede lograrse de manera efectiva mediante un esfuerzo conjunto entre el Estado y la economía. En el marco de una cooperación público-privada, denominada UP KRITIS[17], las empresas operadoras, sus asociaciones y las agencias estatales trabajan estrechamente de forma conjunta, intercambian información sobre amenazas cibernéticas y promueven el desarrollo de estándares de seguridad de TI específicos para cada sector. El objetivo central de UP KRITIS es aumentar la resiliencia de las IC, y en particular la resiliencia de las IC relacionadas con las tecnologías de la información y comunicación, y estabilizarlas en un nivel alto, apropiado a la importancia de la concreta IC.

Con UP KRITIS, la República Federal de Alemania dispone de un instrumento que permite actuar rápidamente en caso de crisis y entender la gestión de la crisis como una tarea conjunta de la economía y el Estado. Desde

[17] UP KRITIS significa Plan de Implementación KRITIS (Umsetzungsplan KRITIS). Se trata, como se ha dicho, de una cooperación público-privada entre los operadores de IC, sus asociaciones y las agencias estatales responsables (Beucher *et al.,* 2023: 503; Bundesamt für Sicherheit in der Informationstechnik. Geschäftsstelle Up Kritis, 2014).

su lanzamiento oficial en el año 2007, la colaboración conocida como UP KRITIS viene realizando una contribución significativa a la prestación confiable de servicios críticos para la población en Alemania. El enfoque se centra en la interacción efectiva de la seguridad de las tecnologías de la información y la comunicación y el mantenimiento de procesos comerciales considerados como críticos. El principio rector de UP KRITIS es la cooperación de los operadores de IC con las agencias estatales para fortalecer la competencia de la economía alemana y del Gobierno federal en la responsabilidad conjunta, en particular en materia de seguridad informática en los procesos de IC.

Ahora bien, en los últimos años ha quedado claro, también en el caso de Alemania, que considerar *por separado* la seguridad física y la seguridad cibernética no es suficiente para lograr el objetivo común de proteger las IC. La cooperación de todos los actores relevantes resulta por tanto esencial para el éxito de las medidas y proyectos destinados a garantizar la seguridad de los procesos críticos, es decir, la colaboración de los departamentos especializados en TI y seguridad informática con los expertos en protección física, para con ello mantener los procesos de producción y suministro, así como la gestión de una eventual crisis.

A partir de lo que se acaba de señalar, en los siguientes epígrafes se va a analizar la legislación aprobada (o pendiente de aprobación) en Alemania con el objetivo de proteger las IC. Como se verá a continuación, dicha legislación ha pasado de estar enfocada casi de forma exclusiva a garantizar la resiliencia frente a amenazas provenientes del mundo cibernético, a contemplar también la necesidad de protección física frente a amenazas procedentes de desastres naturales o de la mano del hombre.

2. LOS COMIENZOS (BSI-GESETZ Y BSI-KRITISV)

Además de otras regulaciones, las disposiciones en materia de seguridad informática han venido estando en Alemania en el centro de las actividades legislativas debido a la dependencia de las IC de las tecnologías de la información y la comunicación, en particular del uso de Internet.

La primera ley que en este sentido merece ser destacada es la Ley de la Oficina Federal de Seguridad de la Información (BSI-Gesetz)[18]. A lo que este trabajo interesa, esta ley especifica, en primer lugar, los sectores en los que las

[18] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG), de 14 de agosto de 2009 (*Boletín Oficial Federal* [*Bundesgesetzblatt, BGBl.* en lo sucesivo] I, p. 2821).

instalaciones pueden ser clasificadas como IC, así como los requisitos generales para la existencia de una IC. En concreto, el parágrafo § 2, apdo. 10, BSI-Gesetz contiene el siguiente tenor literal:

> Se consideran infraestructuras críticas, a los efectos de la presente Ley, las instalaciones, plantas o partes de las mismas que 1. pertenezcan a los sectores de la energía, la tecnología de la información y las telecomunicaciones, el transporte y el tráfico, la salud, el agua, la alimentación, las finanzas y los seguros, así como la eliminación de residuos de áreas residenciales, y 2. son de gran importancia para el funcionamiento de la comunidad porque su caída o deterioro traería consigo importantes cuellos de botella en el suministro o bien amenazas a la seguridad pública. Las infraestructuras críticas en el sentido de esta Ley son definidas con más detalle en el Reglamento, de conformidad con el § 10 apartado 1.

Qué servicios de los ocho sectores enunciados en el mencionado precepto se consideran críticos por su importancia y qué nivel de prestación resulta relevante en cada caso están regulados en un reglamento sobre la base del § 10, apdo. 1, BSI-Gesetz. En efecto, el 22 de abril de 2016, el Ministerio del Interior aprobó el Reglamento sobre la Determinación de Infraestructuras Críticas según la Ley BSI (BSI-KritisV), el cual entró en vigor el 3 de mayo de 2016[19]. Posteriormente, el 21 de junio de 2017 se aprobó el Primer Reglamento para la reforma del BSI-KritisV, el cual entró en vigor el 30 de junio de 2017.

La determinación de si una empresa, como operadora de una IC, está sujeta a las obligaciones de la BSI-Gesetz u otras leyes especiales se realiza de acuerdo con los siguientes criterios:

1. En primer lugar, es necesario examinar si la empresa ofrece la prestación de un servicio considerado como crítico.
2. Si se ofrece un servicio considerado como crítico, se debe comprobar si para proporcionar ese servicio se utiliza una instalación *(Anlage)* o parte de una instalación, la cual se puede incluir en una de las categorías de instalaciones especificadas en la BSI-Gesetz.
3. Si también ello es así, se deberá entonces determinar el nivel de suministro de la instalación. Si el mismo excede el denominado «valor umbral» *(Schwellenwert)* para la categoría de instalación correspondiente, el operador está sujeto a las obligaciones establecidas en la BSI-Gesetz (o las disposiciones legales especiales correspondientes) (Beucher *et al.,* 2023: 509-510).

[19] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritsV), de 22 de abril de 2016 (*BGBl.* I, p. 958).

Como se ha señalado anteriormente, el Reglamento de la BSI-Gesetz (BSI-KritisV) determina para los ocho sectores que principalmente se consideran como IC (energía, agua, alimentación, tecnología de la información y telecomunicaciones, salud, finanzas y seguros, transporte y tráfico, eliminación de residuos de áreas residenciales), aquellos servicios que deben considerarse críticos debido a su importancia, así como las correspondientes instalaciones críticas *(kritische Anlagen)* (Beucher *et al.,* 2023: 515).

Aunque la energía nuclear desempeña un papel cada vez más reducido en Alemania, la misma seguirá perteneciendo al sector KRITIS hasta su desmantelamiento definitivo. Incluso después de que eso ocurra, resulta pertinente una protección reforzada. Porque debe garantizarse un tratamiento seguro de las sustancias radiactivas y de los productos finales; y esto debe continuar durante muchas décadas después del desmantelamiento de las centrales nucleares[20]. Si bien no se va a analizar en el presente trabajo, conviene apuntar que la energía nuclear es objeto en Alemania de una regulación específica, en concreto mediante la Ley sobre el uso pacífico de la energía nuclear y la protección contra sus peligros (Ley de Energía Atómica, *Atomgesetz*), de 15 de julio de 1981. También, con respecto a la energía nuclear y las centrales nucleares, y desde el punto de vista de la protección frente a amenazas, hay que tener en cuenta la Directriz para la protección de los sistemas informáticos en las instalaciones nucleares y para las actividades de la categoría de seguridad III, así como para la gestión operativa prudente frente a medidas disruptivas u otras influencias de terceros (Directriz SEWD IT SK III, de 21 de septiembre de 2020). El texto de la Directriz no se publica debido a su consideración como información clasificada (Bundesamt für die Sicherheit der nuklearen Entsorgung, 2020). SEWD es el acrónimo (en alemán) de «protección contra medidas disruptivas y otras influencias de terceros durante la manipulación y transporte de otras sustancias radiactivas».

Es importante reseñar que el Reglamento sobre la Determinación de Infraestructuras Críticas según la BSI-Gesetz (BSI-KritisV) no califica *per se* determinadas empresas o ubicaciones operativas como IC, sino únicamente instalaciones *(Anlagen).* Si una empresa ofrece la prestación de un servicio considerado como crítico, solo está sujeta a la regulación como IC si para brindar el servicio opera una instalación o una parte de la misma. El Regla-

[20] Sobre el desmantelamiento de la energía nuclear en Alemania, véase: «"El fin de una era": Alemania abandona la energía nuclear tras más de 60 años pese a las presiones por la guerra de Ucrania», *BBC-News Mundo,* edición *online* de 16 de abril de 2023. Disponible en: https://is.gd/lsOeSg.

mento de la BSI-Gesetz enumera las correspondientes categorías de instalaciones en los anexos 1 a 7.

De acuerdo con el § 1 núm. 1 BSI-KritisV, se consideran instalaciones *(Anlagen):* (a) plantas de operación y otras instalaciones *fijas* que son necesarias para la prestación de un servicio crítico, así como (b) las máquinas, equipos y otras instalaciones *móviles* que son necesarias para la prestación de un servicio crítico.

El destinatario de las obligaciones de la BSI-Gesetz es el operador de la instalación de IC. De acuerdo con el § 1 núm. 2 BSI-KritisV, un operador es «una persona física o jurídica que, teniendo en cuenta las circunstancias jurídicas, económicas y fácticas, ejerce una influencia decisiva sobre la condición y el funcionamiento de una instalación o de partes de la misma». Si el operador subcontrata partes de la IC a terceros, la responsabilidad de implementar las obligaciones según la BSI-Gesetz sigue siendo suya. Esto se aplica, por ejemplo, cuando los sistemas de tecnología de la información se subcontratan a un proveedor de servicios, siempre que el operador no renuncie con ello a su influencia decisiva sobre la concreta instalación (Beucher *et al.,* 2023: 517).

La parte más importante de la BSI-Gesetz es aquella que hace referencia a las obligaciones de los operadores de la instalación de una IC. Como se verá a continuación, dichas obligaciones se centran, sobre todo, en garantizar la seguridad en el ámbito de la tecnología de la información. Así, según se establece en el § 8a BSI-Gesetz, los operadores de IC deben garantizar la seguridad de sus sistemas de tecnología de la información.

Entre las obligaciones impuestas cabe destacar las siguientes: (1) Precauciones de seguridad apropiadas de acuerdo con el estado de la técnica o los estándares de seguridad específicos de cada sector y otras especificaciones del estado de la técnica. (2) Obligaciones de comprobación periódicas. De acuerdo con el § 8a, apdo. 3, BSI-Gesetz, los operadores de IC deben demostrar el cumplimiento de los requisitos establecidos en el § 8, apdo. 1, BSI-Gesetz cada dos años. La prueba de que se han llevado a cabo las pertinentes comprobaciones puede proporcionarse mediante auditorías de seguridad, inspecciones o certificaciones. El operador deberá remitir a la BSI los resultados de las comprobaciones, así como las notificaciones sobre cualquier deficiencia de seguridad detectada. (3) Obligación de designar y registrar una oficina de contacto (§ 8b, apdo. 3, BSI-Gesetz), garantizando así que se pueda contactar con ellos en cualquier momento a través de esa oficina de contacto. Las averías deben notificarse a través de la oficina de contacto de conformidad con lo establecido en el § 8b, apdo. 4, BSI-Gesetz. (4) Obligaciones de informar en caso de averías (§ 8b, apdo. 4, BSI-Gesetz). Los operadores de IC deben informar inmediatamente a la BSI sobre determi-

nadas averías en sus sistemas de tecnología de la información. La obligación de informar no solo existe cuando se ha producido una avería; incluso la posibilidad de una caída del sistema puede dar lugar a una obligación de informar. La BSI recopila estos informes, los evalúa, analiza las posibles repercusiones de las averías en la disponibilidad de la IC y crea un informe de situación. Una avería «común» se produce, entre otras cosas, cuando «la tecnología utilizada ya no puede cumplir adecuada o completamente su función prevista […]» (§ 8b, apdo. 4, frase 1, núm. 1 BSI-Gesetz). Una avería «significativa» existe en el sentido del § 8b, apdo. 4, frase 1, núm. 2 BSI-Gesetz cuando «la funcionalidad del servicio prestado está amenazada». (5) Cooperación con la BSI en caso de averías significativas. Durante una avería significativa, la BSI, de común acuerdo con la autoridad supervisora federal pertinente[21], puede exigir a los operadores de IC afectados que proporcionen la información necesaria para abordar y controlar la avería, incluidos los datos personales. Sobre esta base, la BSI puede obligar a los operadores de IC a revelar las direcciones de IP necesarias para localizar la fuente de la avería, o los correos electrónicos si los mismos contienen *malware* y la BSI necesita analizarlos para valorar la naturaleza de la avería.

Conviene señalar que con la Ley de Seguridad Informática del año 2015[22] y su desarrollo posterior, a saber, la Ley de Seguridad Informática 2.0 del año 2021[23], existe también en Alemania un marco legal establecido para regular la ciberseguridad en el ámbito de las IC. La ciberseguridad de las IC se sincroniza también estrechamente con los requisitos legales europeos procedentes de la Directiva de seguridad de las redes y sistemas de infor-

[21] Hay que decir que ni la propia BSI-Gesetz ni su exposición de motivos aclaran qué otras autoridades de control son responsables a este respecto.

[22] Ley para aumentar la seguridad de los sistemas de tecnología de la información (Ley de Seguridad Informática, IT-SiG, por sus siglas en alemán), de 17 de julio de 2015 (*BGBl.* I, 1324) (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme [IT-Sicherheitsgesetz]). Con la IT-SiG y la Directiva (EU) 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 (NIS-RL), tanto el legislador alemán como el europeo han previsto medidas obligatorias para lograr un nivel uniforme de seguridad para las redes y los sistemas de información de determinadas IC (Beucher *et al.,* 2023: 503).

[23] Con la Segunda Ley para aumentar la seguridad de los sistemas de tecnología de la información (Ley de Seguridad Informática 2.0), de 18 de mayo de 2021 (IT-SiG 2.0, por sus siglas en alemán), y que entró en vigor el 28 de mayo de 2021, el legislador alemán ha creado nuevas regulaciones para los operadores de IC, ampliando las ya existentes.

mación de la UE (Directiva NIS de la UE), así como la nueva Directiva NIS-2 de la UE (Der Beauftrage der Bundesregierung für Informationstechnik, s. f.).

Pues bien, desde la entrada en vigor de la IT-SiG 2.0, además de las IC y los servicios digitales, las llamadas «empresas de especial interés público» *(Unternehmen im besonderen öffentlichen Interesse)* también están sujetas a obligaciones especiales de seguridad informática y de comunicación según la BSI-Gesetz, las cuales resultan comparables a las de los operadores de IC, pero que sin embargo no alcanzan su intensidad. El § 2, apdo. 14, BSI-Gesetz define el término «empresas de especial interés público» dividiéndolas en tres categorías: (1) las empresas con actividad en la industria armamentística y los fabricantes de productos informáticos para procesar información clasificada estatal; (2) las empresas de particular importancia económica; (3) los operadores de un área operativa de nivel superior en el sentido del Reglamento sobre Accidentes Graves (Störfall-Verordnung).

3. LA TRANSPOSICIÓN DE LAS DIRECTIVAS 2022/2555 Y 2022/2557 AL ORDENAMIENTO JURÍDICO ALEMÁN

3.1. Proyecto de ley de 7 de mayo de 2024 (NIS-2-RL)

En mayo del año 2024, el Gobierno alemán se puso manos a la obra para llevar a cabo la transposición de la Directiva 2022/2055, para lo cual presentó un proyecto de ley de transposición de la conocida como Directiva NIS-2[24]. El objetivo de este proyecto, además de dar cumplimiento a los requisitos procedentes del derecho de la UE, era ampliar el marco normativo con el punto de mira puesto en fortalecer la ciberseguridad de las IC Hay que recordar al respecto que, junto a la BSI-Gesetz y el BSI-KritisV —analizadas anteriormente— en Alemania se encontraban ya en vigor la Ley de Seguridad Informática (IT-SiG) de 17 de julio de 2015 y la Segunda Ley para aumentar la seguridad de los sistemas de la tecnología de la información (Ley de Seguridad Informática 2.0, IT-SiG 2.0, por sus siglas en alemán), de 18 de mayo de 2021. Con el proyecto de ley de mayo de 2024, además de fortalecer

[24] Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz), de 7 de mayo de 2024 (OpenKRITIS, 2024). Debido a la convocatoria de elecciones anticipadas en Alemania, celebradas el pasado 23 de febrero de 2025, no se pudo completar en su momento el trámite parlamentario de este proyecto de ley.

la ciberresiliencia de las IC existentes en Alemania, se introducían también disposiciones correspondientes en el ámbito de la administración federal.

Particularmente, las reformas que pretendía llevar a cabo el mencionado proyecto de ley son las siguientes:

1. Introducción de las categorías de entidades (instalaciones) especificadas por la Directiva NIS-2, lo que supone una importante ampliación del ámbito de aplicación anteriormente limitado a los operadores de IC, proveedores de servicios digitales y empresas de especial interés público[25].
2. Incorporación a la BSI-Gesetz del catálogo de requisitos mínimos de seguridad del art. 21, apdo. 2, de la Directiva NIS-2, si bien, por razones de proporcionalidad, se diferencia la intensidad de la respectiva medida entre las distintas categorías.
3. La anterior obligación de notificación de incidentes en una sola etapa es reemplazada por el régimen de notificación en tres etapas previsto en la Directiva NIS-2. El objetivo es minimizar la carga burocrática de las entidades en el marco del margen de ejecución existente de que disponen los Estados miembros.
4. Ampliación de las herramientas a disposición de la Oficina Federal de Seguridad de la Información (BSI) en relación con las medidas de supervisión especificadas en la Directiva NIS-2.
5. Anclaje jurídico de las exigencias nacionales esenciales con respecto a la gestión de la seguridad de la información de la República Federal

[25] En concreto, la Directiva 2022/2555 señala en su punto 15 lo siguiente: «Las entidades incluidas en el ámbito de aplicación de la presente Directiva a efectos del cumplimiento de las medidas para la gestión de riesgos de ciberseguridad deben clasificarse en dos categorías, entidades esenciales y entidades importantes, en función del grado de criticidad de sus sectores o del tipo de servicio que prestan, así como de su tamaño». Al respecto, se consideran entidades esenciales aquellas de naturaleza económica o social que resultan esenciales para el funcionamiento de un país, como por ejemplo las infraestructuras clave en sectores como la energía, el transporte, la sanidad o la infraestructura digital. En caso de que estos sectores fueran víctimas de un ciberataque, ello podría tener consecuencias de alta gravedad para la sociedad, la economía o incluso la seguridad nacional. Por su parte, las entidades importantes son aquellas cuya actividad resulta relevante para la economía y la sociedad, pero cuyo impacto por interrupciones no es tan crítico como en el caso de las entidades esenciales. En este grupo se incluyen, por ejemplo, los proveedores de servicios postales y de mensajería o los sectores dedicados a la producción, transformación y distribución de alimentos.

alemana *(Bund)* y mapeo de los roles y responsabilidades asociados (OpenKRITIS, 2024).

Tal y como se ha señalado *supra,* el pasado mes de diciembre del año 2025 el aquí analizado proyecto de ley desembocó finalmente en la aprobación de la Ley de transposición de la Directiva NIS-2 y de regulación de los principios esenciales de la gestión de la seguridad de la información en la Administración Federal[26]. Con ello, el legislador germano ha logrado finalmente transponer la Directiva 2022/2555 a su ordenamiento jurídico interno.

3.2. Proyecto de ley de 6 de noviembre de 2024 (CER-RL)

Como se señaló anteriormente, el 16 de enero de 2023 entró en vigor la Directiva 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas (Directiva CER). En consecuencia, el Estado alemán se puso también manos a la obra para cumplir con las prerrogativas procedentes de la UE de cara a la transposición de dicha normativa al ordenamiento interno de los Estados miembros.

En primer lugar, el entonces Ministerio del Interior y de la Patria aprobó en su seno un proyecto de ley *(Referentenentwurf)* con fecha de 21 de diciembre de 2023[27]. Posteriormente, el 6 de noviembre de 2024 se aprobó el correspondiente proyecto de ley gubernamental dirigido a la transposición de la Directiva 2022/2557[28]. En lo que sigue, la explicación va a seguir lo regulado tanto en el proyecto ministerial como en el proyecto de ley del Gobierno federal.

El aspecto sin duda más importante de la normativa germana dirigida a la transposición de la Directiva 2022/2557 es la creación de un cuerpo legislativo autónomo cuyo objetivo es apuntalar jurídicamente la protección integral de las IC en Alemania. Se trata de la denominada Ley paraguas KRITIS (KRITIS-Dachgesetz). Conviene recordar al respecto que, con el objetivo de fortalecer la

[26] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, de 5 de diciembre de 2025 (*BGBl.* 2025 I Nr. 301), encontrándose en vigor desde el 6 de diciembre de 2025. La mencionada ley también es conocida como NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG). Véase al respecto Lämmerhit (2025).

[27] Referentenentwurf des Bundesministeriums des Innern und für Heimat. Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen, de 21 de diciembre de 2023.

[28] Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen, de 6 de noviembre de 2024.

resiliencia de las entidades críticas, la Directiva 2022/2557 creó un marco general («paraguas»), el cual, en el sentido de un enfoque de todos los peligros, tiene en cuenta los peligros naturales o los peligros provocados por el hombre, ya sean estos accidentales o intencionados. Pues bien, concretando este marco general establecido en el ámbito de la UE, la Ley paraguas KRITIS señala al principio que la gama de infraestructuras críticas es amplia, los peligros son diversos y abarcan desde desastres naturales y pandemias, pasando por ataques en el contexto de amenazas híbridas, errores humanos, terrorismo y sabotaje, hasta un suministro inadecuado de los recursos necesarios, por ejemplo, debido al colapso de las cadenas de suministro. Los fallos y las interrupciones de las IC pueden generar cuellos de botella en el suministro y perturbaciones importantes en la seguridad y el orden públicos.

La Ley paraguas para el fortalecimiento de la resiliencia física de las IC[29] (KRITIS-Dachgesetz) complementará las demás regulaciones existentes para la resiliencia de los sistemas críticos según el «enfoque de todos los riesgos» *(All-Gefahren-Ansatz),* poniendo, eso sí, el foco en la protección física, para distinguirla de la seguridad informática. En el contexto de una normativa incoherente o inexistente para la protección *física* de las IC y en vista de las dependencias intersectoriales y transfronterizas en el conjunto del territorio alemán, la Ley paraguas KRITIS tiene en cuenta por primera vez todo el sistema de protección física de las IC en Alemania, regulándolo por ley en el marco de las competencias asignadas al Gobierno federal. La Ley paraguas KRITIS complementa así la normativa existente sobre ciberprotección de las IC, contribuyendo de esta manera a crear un sistema coherente y resiliente, a la vez que una protección holística e híbrida de las IC y de las entidades importantes y esenciales[30].

Debe tenerse en cuenta que con la transposición al ordenamiento jurídico alemán de la Directiva NIS-2 se ampliará el conjunto ya en sí extenso de reglas existentes para proteger la seguridad de las IC en el ámbito de las tecnologías de la información y comunicación, mientras que, con respecto a las medidas de resiliencia física, esta ley, con la implementación de la Directiva 2022/2557, introducirá por vez primera regulaciones independientes e intersectoriales. Por lo tanto, el ámbito de aplicación de la Ley paraguas KRITIS es más

[29] Conviene señalar en este punto que, si bien la Directiva 2022/2557 hace referencia explícita a las entidades críticas, la Ley paraguas KRITIS, a lo largo de su articulado, se refiere a las allí denominadas *kritische Infrastrukturen,* lo cual debe traducirse como «infraestructuras críticas». Es por ello que aquí se ha optado por mantener la nomenclatura empleada por el legislador germano.

[30] Véase al respecto la nota n.º 25.

pequeño y la intensidad regulatoria menor que con respecto a las regulaciones destinadas a la transposición de la Directiva NIS-2.

La Ley paraguas KRITIS no contiene ninguna regulación específica para ningún sector o industria, sino que estipula, en abstracto, que los operadores de instalaciones críticas en todos los sectores de KRITIS deben tomar medidas apropiadas y proporcionadas para garantizar la protección física de las IC. Para ello, la Ley paraguas KRITIS establece un proceso que incluye, en particular, evaluaciones de riesgos nacionales y con respecto a los operadores en todos los sectores, la preparación de planes de resiliencia por parte de los operadores y el desarrollo de normas de resiliencia específicas para cada sector por parte de las asociaciones comerciales en los diversos sectores.

La KRITIS-Dachgesetz contiene disposiciones para la identificación de IC, que se especifican con más detalle en un reglamento, así como para su registro. Los operadores de instalaciones críticas que prestan servicios críticos en o para al menos seis Estados miembros de la Unión Europea, se identifican como entidades críticas de especial importancia para Europa, estando sujetas a medidas especiales. Los operadores de IC deberán tomar medidas para fortalecer su resiliencia. Esto incluye el desarrollo y la implementación de planes de resiliencia que, sobre la base de análisis de riesgos y evaluaciones de riesgos realizados por los operadores, describen qué medidas técnicas, organizativas y de seguridad, apropiadas y proporcionadas, se están adoptando para fortalecer la resiliencia[31]. La Ley paraguas KRITIS contiene objetivos de resiliencia que los operadores de instalaciones críticas deben alcanzar con sus medidas, así como, con fines de orientación, una descripción general ejemplificativa de las medidas que pueden adoptar los operadores. Con ello, la Ley paraguas KRITIS regula por vez primera en el ordenamiento federal los requisitos mínimos uniformes e intersectoriales en lo que respecta a medidas no relacionadas con las tecnologías de la información y comunicación, para con ello fortalecer la resiliencia de los operadores de instalaciones críticas.

Las amenazas a las IC están sujetas a una evaluación periódica. Las evaluaciones de riesgos realizadas por el Estado en relación con los servicios críticos proporcionarán a los operadores una base para sus propias evaluaciones de riesgos específicas y periódicas, así como las acciones basadas en ellas. Mediante estas evaluaciones de riesgos se aumenta sistemáticamente la conciencia sobre los

[31] Cabe recordar al respecto que el art. 4 de la Directiva 2022/2557 establece que, antes del 17 de enero de 2026, se adoptará una estrategia nacional para mejorar la resiliencia de las IC (Estrategia Nacional de Resiliencia KRITIS). Al respecto, el § 1 KRITIS-Dachgesetz señala lo siguiente: «A más tardar el 17 de enero de 2026, el Gobierno Federal adoptará una estrategia para mejorar la resiliencia de las infraestructuras críticas».

peligros. Con ello se tienen en cuenta todos los riesgos naturales y provocados por el hombre, así como los riesgos intersectoriales[32] y transfronterizos. Las evaluaciones de riesgos se llevarán a cabo periódicamente al menos cada cuatro años.

Por otro lado, la protección de las IC es una tarea interdepartamental, de carácter nacional y que se sitúa por encima de los actores involucrados. Los operadores de IC, ya sean empresas privadas o instituciones públicas, deben garantizar su funcionalidad. El enfoque cooperativo se complementa con la Ley paraguas KRITIS mediante normas de protección obligatorias para la seguridad física. Esto proporciona a los operadores mayor orientación y seguridad en sus actuaciones.

Las interrelaciones y dependencias de las IC se tienen también en cuenta a nivel administrativo. En un nuevo enfoque, la protección física de las IC se considera un tema independiente dentro de la Ley paraguas KRITIS, siendo esa protección física coordinada por una autoridad competente general. También se tienen en cuenta las repercusiones transfronterizas mediante una cooperación aún más estrecha dentro de un marco europeo. Para ello, la Oficina Federal de Protección a la Población y Ayuda en caso de Catástrofes (BBK, por sus siglas en alemán), dependiente del actual Ministerio del Interior, será ampliada para convertirse en el organismo general responsable de la protección física de las IC en el marco de los recursos presupuestarios disponibles. Una autoridad general competente y responsable como la prevista es necesaria para el objetivo que se persigue con la Ley paraguas KRITIS de considerar el sistema en su totalidad. La BBK ya dispone de una amplia experiencia metodológica e intersectorial en este ámbito. La BBK trabajará en estrecha colaboración con la Oficina Federal de Seguridad de la Información (BSI), en particular para lograr coherencia en la protección *cibernética* y la protección *física* de las IC (Bundesministerium des Innern und für Heimat, 2022a). Los operadores de IC están obligados a informar de inmediato a una oficina de notificación conjunta creada por la BBK y la BSI sobre los incidentes que alteren o puedan alterar significativamente la prestación de servicios críticos (Kipker, 2024)[33]. El nuevo sistema de comunicación que se introduce en el área de la seguridad física complementa el sistema de comunicación ya existente en el ámbito de la ciberseguridad de las IC. El Estado también

[32] Si se producen fallos en un sector, como el energético, el de la tecnología de la información/telecomunicaciones o el de transporte/tráfico, esto puede tener graves consecuencias para otros sectores.

[33] Conviene recordar en este punto que, en el caso de Alemania, las medidas federales para la protección de IC se coordinan de forma interdepartamental por el Ministerio del Interior.

seguirá apoyando a los operadores mediante análisis, directrices, asesoramiento, ejercicios y formación.

La Ley paraguas KRITIS y la consiguiente transposición de la Directiva 2022/2557, así como la implementación de la Directiva NIS-2 a través de la correspondiente ley de transposición, tienen en cuenta las interfaces entre la seguridad en el contexto de las tecnologías de la información y la comunicación *(IT-Sicherheit)* y la resiliencia física de las IC, armonizando regulaciones y, en la medida de lo posible y razonable, diseñándolas de manera concordante. Las disposiciones adoptadas por la Ley paraguas KRITIS con respecto a los operadores de IC se basan en la normativa anterior sobre seguridad informática de IC, teniendo en cuenta la implementación prevista de la Directiva NIS-2, con el objetivo de facilitar la construcción del sistema para la economía sobre la base del «enfoque de todos los riesgos» *(All-Gefahren-Ansatz)*. Para garantizar la coherencia de las IC en el sentido de la BSI-Gesetz y la Ley paraguas KRITIS, en el futuro los operadores de IC solo estarán determinados por la Ley paraguas KRITIS y la normativa reglamentaria de desarrollo.

Conviene finalmente señalar que el pasado 29 de enero del presente año 2026, el Bundestag ha aprobado finalmente el aquí analizado proyecto de ley de noviembre del año 2024[34], por lo que próximamente verá la luz la ley de transposición de la Directiva (UE) 2022/2557 y de reforzamiento de la resiliencia de las entidades críticas.

IV. LA TRANSPOSICIÓN DE LAS DIRECTIVAS 2022/2555 Y 2022/2557 EN ESPAÑA

1. ANTEPROYECTO DE LEY DE COORDINACIÓN Y GOBERNANZA DE LA CIBERSEGURIDAD, DE 14 DE ENERO DE 2025

En el concreto caso de España, el pasado 14 de enero de 2025, el Consejo de Ministros aprobó el Anteproyecto de Ley de Coordinación y Gobernanza

[34] Véase: «Bundestag beschließt Gesetz zur Stärkung kritischer Anlagen», Deutscher Bundestag, 29 de enero de 2026. Disponible en: https://is.gd/AibxIf. Conviene señalar al respecto que la Comisión de Interior (Innenausschuss) llevó a cabo una pequeña modificación del proyecto gubernamental, dictaminando que los estados federados (Länder) tendrán la opción de identificar otras instalaciones críticas que presten servicios esenciales y que sean exclusivamente de su jurisdicción. Para ello, el Ministerio Federal del Interior está autorizado a emitir un instrumento legal que establezca los criterios y procedimientos aplicables, debiendo dicho instrumento ser aprobado por el Bundesrat (Cámara Alta).

de la Ciberseguridad[35]. El objetivo último de esta norma es 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. Cuando sea aprobada de manera definitiva, la futura ley incorporará al ordenamiento jurídico español la Directiva 2022/2555, de 14 de diciembre de 2022, conocida como NIS-2. El Ministerio del Interior comunicó de inmediato la aprobación de este anteproyecto a la Comisión Europea, dado que el plazo para la transposición de la Directiva NIS-2 al derecho interno español había vencido el 17 de octubre de 2024 (Ministerio del Interior, 2025).

El objetivo principal de la ley es establecer medidas para alcanzar un elevado nivel común de ciberseguridad en España y contribuir con ello a la ciberseguridad de la UE (art. 1). A tal fin, se establecen una serie de obligaciones que requieren, entre otras cosas, la adopción de una Estrategia Nacional de Ciberseguridad y la designación o establecimiento de autoridades competentes para la gestión de crisis de ciberseguridad, así como equipos de respuesta a incidentes de seguridad informática. El anteproyecto también regula medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades reguladas en la ley, así como normas y obligaciones relativas al intercambio de información sobre ciberseguridad.

El anteproyecto de enero de 2025 consta de cincuenta artículos, estructurados en siete capítulos, así como de ocho disposiciones adicionales, tres disposiciones transitorias, una disposición derogatoria y cinco disposiciones finales.

En cuanto al ámbito de aplicación y los sectores considerados como críticos, la propia Directiva (UE) 2022/2555 establece —como se señaló anteriormente— un criterio uniforme para determinar qué entidades están incluidas en su ámbito de aplicación y, por lo tanto, deben cumplir las medidas contempladas para la gestión de riesgos de ciberseguridad. A tal fin, las entidades se clasifican en dos categorías: entidades esenciales y entidades importantes, en función del grado de criticidad de sus sectores o del tipo de servicio que prestan, así como de su tamaño[36]. En el concreto caso del anteproyecto español del año 2025, el art. 3, apdo. 1, señala que la ley resulta de aplicación a las entidades públicas y privadas que tengan su residencia fiscal en España y que se encuentren dentro de los sectores de alta criticidad y otros

[35] Ministerio del Interior (2025a). Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.

[36] Véase al respecto la nota n.º 25.

sectores críticos recogidos en los anexos I y II[37], cuando tengan la consideración de medianas o grandes empresas porque cuentan con cincuenta o más trabajadores, y tengan un volumen de negocios anual o un balance general anual que supera los diez millones de euros.

Dentro del marco estratégico e institucional (arts. 5 a 13 del anteproyecto), resulta de capital importancia hacer referencia a la Estrategia Nacional de Ciberseguridad (ENC). Tal y como se establece en el art. 5, la ENC tiene como objetivo prioritario establecer los objetivos estratégicos, los recursos necesarios y las medidas políticas y normativas adecuadas para alcanzar y mantener un elevado nivel de ciberseguridad. Para ello, el propio art. 5 hace referencia, entre otras, a las siguientes cuestiones objeto de abordaje por la ENC: (1) las medidas estratégicas necesarias para garantizar la preparación, la capacidad de respuesta y la recuperación frente a incidentes; (2) el marco de actuación para la coordinación con las autoridades competentes designadas conforme a la ley encargada de transponer al ordenamiento jurídico español la Directiva (UE) 2022/2557[38], a efectos del intercambio de información sobre los riesgos, las ciberamenazas e incidentes, así como sobre riesgos, amenazas e incidentes no relacionados con la ciberseguridad y el ejercicio de las funciones de supervisión[39]; (3) un plan de medidas para mejorar la concienciación de los ciudadanos en materia de ciberseguridad.

---

[37] El anexo I enumera lo que denomina «Sectores de alta criticidad», y que son los siguientes: (1) energía; (2) transporte; (3) banca; (4) infraestructuras de los mercados financieros; (5) sector sanitario; (6) agua potable; (7) aguas residuales; (8) infraestructura digital; (9) gestión de servicios de TIC (de empresa a empresa); (10) entidades de la Administración pública, con exclusión del poder judicial, los parlamentos y los bancos centrales; (11) espacio; (12) industria nuclear. Por su parte, el anexo II realiza un listado que incluye los siguientes «otros sectores»: (1) servicios postales y mensajería; (2) gestión de residuos; (3) fabricación, producción y distribución de sustancias y mezclas químicas; (4) producción, transformación y distribución de alimentos; (5) fabricación de distintos productos, materiales, vehículos y maquinaria enumerados en el propio anexo II; (6) proveedores de servicios digitales; (7) investigación; (8) seguridad privada.

[38] En este caso, el anteproyecto que aquí se analiza está haciendo referencia al posterior Anteproyecto de Ley de Protección y Resiliencia de Entidades Críticas, de 27 de mayo de 2025, el cual será analizado *infra.*

[39] Para fortalecer esta coordinación entre seguridad física y cibernética, el propio anteproyecto establece por un lado que las entidades que hayan sido identificadas como críticas en el contexto de la Directiva (UE) 2022/2557 deben también ser consideradas entidades esenciales a los efectos del anteproyecto; por otro, que las obligaciones impuestas a las entidades pertenecientes al sector de las infraestructuras digitales

Sobre la base de la citada ENC, en el mismo capítulo tercero se regulan las concretas medidas para la gestión de riesgos de ciberseguridad y las obligaciones de notificación (arts. 14 a 25). Así, en esta parte del anteproyecto se contempla, entre otras cosas, la realización de una evaluación individualizada del riesgo por parte de las distintas entidades, detallándose las actuaciones a llevar a cabo por estas para garantizar y elevar sus niveles de seguridad de las redes y sistemas de información y prevenir el riesgo de incidentes, así como la obligación de notificar a la correspondiente autoridad de control los incidentes significativos que se produzcan en su operativa o en la prestación de sus servicios. Tal y como se establece en el art. 18, apdo. 2, las notificaciones que realicen las entidades esenciales o importantes se referirán a los incidentes que afecten a las redes y sistemas de información empleados en su operativa o en la prestación de sus servicios, tanto si son redes y servicios propios, como si pertenecen a proveedores externos. Para dar cumplimiento a las obligaciones de notificación se pondrá a disposición de todos los actores involucrados la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (art. 19), que permitirá el intercambio de información técnica y el seguimiento de incidentes.

En virtud de lo establecido en el art. 16 del anteproyecto, las entidades esenciales e importantes designarán a una persona, unidad u órgano colegiado como responsable de la seguridad de la información, el cual ejercerá las funciones de punto de contacto y coordinación técnica con las autoridades de control y con los equipos de respuesta a incidentes de ciberseguridad nacionales de referencia, los cuales serán analizados *infra.* El responsable de la seguridad de la información tiene, entre otras, las siguientes funciones: (1) supervisar y desarrollar la aplicación de las políticas de seguridad, y procedimientos derivados de la organización, su efectividad y llevar a cabo controles periódicos de seguridad; (2) supervisar el cumplimiento de la normativa aplicable en materia de seguridad de las redes y sistemas de información; (3) remitir a las autoridades de control, sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios y de las vulnerabilidades detectadas.

Por lo que hace referencia al marco institucional y de gobernanza, el anteproyecto prevé en su art. 6 la creación del Centro Nacional de Ciberseguridad (CNC). El mismo está concebido como la autoridad nacional competente única en materia de gobernanza de la ciberseguridad, encargándose de la

deben abordar de manera exhaustiva, como parte de sus medidas para la gestión de los riesgos de ciberseguridad y obligaciones de notificación, la seguridad física de las redes y sistemas de información (Ministerio del Interior, 2025a: 5).

dirección, impulso y la coordinación, en el ámbito de la ley, de todas las actividades necesarias para garantizar un elevado nivel de ciberseguridad en España y contribuir con ello a la ciberseguridad de la UE[40]. El CNC ejerce como autoridad nacional de gestión de crisis y «punto de contacto único», asumiendo 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 denominados CSIRT (*computer security incident response team* o equipos de respuesta a incidentes de seguridad informática) nacionales de referencia. Básicamente, como autoridad nacional de gestión de crisis de ciberseguridad, el CNC será responsable de la coordinación para la gestión de incidentes y crisis de ciberseguridad a gran escala[41].

Según se establece en el art. 7 del anteproyecto, son autoridades de control, encargadas de las funciones de supervisión y ejecución a que se refiere el capítulo VI de la ley, las siguientes: (1) el Ministerio de Defensa, a través del Centro Criptológico Nacional para una serie de entidades esenciales e importantes; (2) 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 la Secretaría de Estado de Digitalización e Inteligencia Artificial, para otro conjunto de entidades esenciales e importantes; (3) el Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad de la Secretaría de Estado de Seguridad, para otro conjunto concreto de entidades.

Por su parte, el apdo. 3 del art. 7 del anteproyecto establece que, por cada uno de los sectores relacionados en los anexos I y II, se designará, al menos, un órgano ministerial u organismo o entidad de derecho público vinculado o dependiente de la Administración General del Estado que será, en el marco de sus competencias, el punto de contacto sectorial especializado con el CNC y las autoridades de control.

---

[40] Para ello, el CNC se constituye como punto de contacto único para ejercer una función de enlace que garantice la cooperación transfronteriza con las autoridades pertinentes de otros Estados miembros y, cuando proceda, con la Comisión Europea y la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés) (art. 7, apdo. 2).

[41] Al respecto, la disposición adicional primera del anteproyecto señala lo siguiente: «El Gobierno aprobará, en el plazo máximo de doce meses desde la entrada en vigor de la presente ley, el Real decreto por el que se determine el rango, carácter y estructura administrativa del Centro Nacional de Ciberseguridad, adscrito al Gabinete de la Presidencia del Gobierno, dirigiendo y coordinando bajo una autoridad única el ejercicio de las competencias estatales previstas en esta ley».

Finalmente, y a partir de lo establecido en el art. 9 del anteproyecto, son equipos de respuesta a incidentes de ciberseguridad (CSIRT) nacionales de referencia, en materia de seguridad de las redes y sistemas de información, los siguientes: (1) el CCN-CERT, del Centro Criptológico Nacional; (2) el INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España; (3) el ESPDEF-CERT, del Mando Conjunto del Ciberespacio, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que estos requieran y, necesariamente, en las relativas a incidentes de entidades con incidencia en la defensa nacional.

Finalmente, los capítulos VI y VII se dedican, respectivamente, a la regulación de las funciones de supervisión y ejecución sobre las entidades esenciales e importantes y a la cooperación transfronteriza, así como al desarrollo de las potestades disciplinarias.

A destacar sobre todo es el art. 30 del anteproyecto, donde se señala que las autoridades de control, bajo la superior dirección del CNC, supervisarán y adoptarán las medidas necesarias para garantizar el cumplimiento de lo establecido en la ley. Para ello, se podrán establecer metodologías de supervisión que permitan priorizar dichas funciones aplicando un enfoque basado en el riesgo. En el ejercicio de las funciones de supervisión se podrá requerir a las entidades esenciales e importantes que proporcionen toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad. Además, se podrá solicitar información sobre la aplicación efectiva de su política de seguridad, así como auditar o exigir a la entidad que someta la seguridad de sus redes y sistemas de información a una auditoría por una entidad de certificación del marco de cumplimiento de seguridad.

En cuanto al régimen sancionador (arts. 35 a 50), el art. 35 establece que la responsabilidad por las infracciones previstas en la ley recaerá en las entidades esenciales e importantes autoras del hecho en que consista la infracción. Por su parte, el art. 39 del anteproyecto enumera lo que se considera como infracciones muy graves. Entre las mismas cabe destacar las siguientes: (1) la falta de implantación, sin demora indebida, de las medidas técnicas, operativas y de organización determinadas por el CNC para la gestión de riesgos en la seguridad de las redes y sistemas de información, conforme lo indicado en el art. 15, cuando dicha omisión haya motivado un incidente significativo; (2) el incumplimiento reiterado de la obligación de notificar incidentes significativos según se contempla en el art. 18, considerándose que es reiterado a partir del segundo incumplimiento.

Teniendo en cuenta lo ambicioso del citado anteproyecto, el cual contiene medidas dignas de mención como la ENC y la creación de un organismo específico (el CNC), concebido como la autoridad nacional competente única

en materia de gobernanza de la ciberseguridad, es de lamentar que, entrados ya en el presente año 2026, dicho anteproyecto no haya todavía avanzado en la senda legislativa —como así ha ocurrido en el caso de Alemania—, lo que conduce a que, a día de hoy, siga sin ser transpuesta al ordenamiento jurídico español la Directiva 2022/2555, con todo lo que ello implica si se tiene en cuenta la coyuntura geopolítica actual y las amenazas cibernéticas que se ciernen sobre los países miembros de la UE, incluida España.

2. ANTEPROYECTO DE LEY DE PROTECCIÓN Y RESILIENCIA DE ENTIDADES CRÍTICAS, DE 27 DE MAYO DE 2025

El 27 de mayo de 2025, el Consejo de Ministros, a propuesta del Ministerio del Interior, aprobó el Anteproyecto de Ley de Protección y Resiliencia de Entidades Críticas[42]. Esta iniciativa legislativa surge como respuesta a la necesidad de incorporar al ordenamiento jurídico español la Directiva (UE) 2022/2557, de 14 de diciembre, relativa a la resiliencia de las entidades críticas (Directiva CER), cuya fecha límite de transposición se cumplió el pasado 17 de octubre de 2024. Como a nadie escapa, la aprobación de este anteproyecto se produjo en un contexto de creciente preocupación por la vulnerabilidad de infraestructuras y entidades críticas frente a amenazas de diversa índole, desde fenómenos naturales hasta sabotajes y riesgos tecnológicos. Cabe recordar que, apenas un mes antes de la aprobación del mencionado anteproyecto, España sufrió un apagón masivo de la red eléctrica que afectó durante más de doce horas a toda la península ibérica.

Siguiendo con las premisas contempladas en la Directiva 2022/2557, el anteproyecto del mayo de 2025 tiene por objeto la protección *física* de las entidades críticas, mientras que el anteproyecto de enero de 2025 —dirigido, como se sabe, a transponer la Directiva 2022/2555— establece medidas de protección a nivel de *ciberseguridad*. Tal y como señala el anteproyecto, las entidades críticas son aquellas entidades y organismos, públicos o privados, proveedores de servicios esenciales. Por su condición, las entidades críticas resultan indispensables para mantener las funciones sociales o las actividades económicas vitales, no solo en el ámbito nacional, sino también en el contexto de la Unión Europea (Ministerio del Interior, 2025a: 1)[43].

---

[42] Ministerio del Interior (2025b). Anteproyecto de Ley de Protección y Resiliencia de Entidades Críticas.

[43] Por otro lado, y como acertadamente se señala en el mencionado anteproyecto, la 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

El anteproyecto de mayo de 2025 consta de cuarenta y un artículos, estructurados en cinco capítulos, así como de ocho disposiciones adicionales, una transitoria, una derogatoria y siete finales.

El ámbito de aplicación del anteproyecto se circunscribe a las entidades críticas ubicadas en territorio nacional, vinculadas a los sectores y subsectores estratégicos enumerados en el anexo (art. 3)[44], con exclusión de aquellas que ya se encuentran reguladas por normativa sectorial específica, como las entidades del sector bancario, los mercados financieros y las infraestructuras digitales[45]. También quedan excluidas entidades estatales en el ámbito de la defensa y seguridad, como así establece el art. 3 del anteproyecto en los siguientes términos: «Tampoco se aplicará a las entidades dependientes del Ministerio de Defensa, a las Fuerzas y Cuerpos de Seguridad del Estado ni a los cuerpos de policía de las comunidades autónomas con competencias estatutarias reconocidas y asumidas para la protección de personas y bienes y para el mantenimiento del orden público, que se regirán por su propia normativa».

El propio art. 2 del anteproyecto establece una definición de «entidades críticas» en los siguientes términos: «Entidad u organismo, público o privado, identificada conforme a lo previsto en el artículo 12 como perteneciente a una de las categorías de entidades recogidas en el anexo». También define lo que

---

de mejorar su protección, se centraba exclusivamente en la protección de tales *infraestructuras,* desvinculada por tanto de la *entidad* de la que forman parte. Ello dio lugar a que esta directiva fuese derogada por la Directiva 2022/2557, la cual, como se sabe, se dirige a la protección y resiliencia de las entidades críticas frente a amenazas de carácter físico. Esta última directiva viene a establecer que las entidades que explotan infraestructuras críticas han de estar mejor equipadas para hacer frente a los riesgos que puedan dar lugar a una perturbación en la prestación de servicios esenciales.

44 Así, el anexo del anteproyecto contempla los siguientes sectores considerados estratégicos: (1) energía; (2) transporte; (3) banca; (4) infraestructuras de los mercados financieros; (5) sanidad; (6) agua; (7) infraestructura digital; (8) Administración pública; (9) espacio; (10) producción, transformación y distribución de alimentos; (11) industria nuclear; (12) instalaciones de investigación; (13) industria química; (14) seguridad privada; (15) residuos; (16) seguros.

45 Al respecto, la disposición adicional cuarta del anteproyecto señala lo siguiente: «Las disposiciones contenidas en los artículos 6, 8.1 y 2, 9, 10, 23, 24 y 25 y en el capítulo V, no serán de aplicación a las entidades críticas identificadas conforme a lo dispuesto en el artículo 12, en los sectores bancario, de las infraestructuras de los mercados financieros y de las infraestructuras digitales, definidos conforme al Reglamento (UE) 575/2013, al Reglamento (UE) 648/2012, a la Directiva 2014/65/UE y a la Directiva (UE) 2022/2555, y recogidas en los puntos 3, 4 y 7 del anexo».

debe conocerse como «entidades críticas de especial importancia europea», de la manera siguiente: «Entidad crítica identificada que presta los mismos o similares servicios esenciales a o en seis o más Estados Miembros de la Unión Europea y haya sido notificada conforme a lo previsto en el artículo 24». Dicho precepto define también el concepto de «infraestructura crítica» de la siguiente manera: «Un elemento, instalación, equipo, red o sistema, o parte de un elemento, instalación, equipo, red o sistema, que es necesario para la prestación de un servicio esencial».

En cuanto a los sectores considerados estratégicos, el anteproyecto sigue en el anexo al mismo el listado establecido por la Directiva 2022/2557. La identificación de entidades críticas dentro de estos sectores se realizará en función de criterios como el número de usuarios afectados, la interdependencia con otros sectores, la cuota de mercado, la zona geográfica de influencia y la importancia para el mantenimiento de los servicios esenciales.

El anteproyecto introduce un conjunto de medidas y obligaciones dirigidas a fortalecer la protección y resiliencia de las entidades críticas frente a amenazas físicas, naturales y de origen humano. El marco de planificación e implementación de dichas medidas y obligaciones se articula en torno a la Estrategia Nacional para la Protección y Resiliencia de las Entidades Críticas, así como la Evaluación Nacional de Amenazas y Riesgos, ambos documentos elaborados y aprobados por la Secretaría de Estado de Seguridad. Sobre esta base, se desarrollan el Plan Nacional de Protección y Resiliencia de Entidades Críticas, los planes estratégicos sectoriales y los planes de apoyo operativos, estos últimos elaborados por las fuerzas y cuerpos de seguridad en relación con cada infraestructura crítica en su demarcación territorial.

La mencionada estrategia establecerá objetivos estratégicos y medidas de actuación, basándose en estrategias nacionales y sectoriales, planes o documentos similares existentes en la materia, con la finalidad de alcanzar y mantener un alto nivel de resiliencia por parte de las entidades críticas. Los elementos que deberá contemplar dicha estrategia vienen enumerados en el propio art. 4 del anteproyecto. Dicha estrategia se actualizará, como mínimo, cada cuatro años.

Según señala el citado art. 4 del anteproyecto, la Secretaría de Estado de Seguridad utilizará la Evaluación Nacional de Amenazas y Riesgos como instrumento para identificar las entidades críticas y ayudarlas a adoptar medidas adecuadas y proporcionadas para garantizar su resiliencia. Será objeto de actualización y modificación siempre que sea necesario y, como mínimo, cada cuatro años.

El anteproyecto prevé también la creación de un catálogo nacional de entidades críticas y estratégicas, el cual será revisado también, al menos, cada cuatro años. Este catálogo identificará a las organizaciones cuya actividad

resulta indispensable para el mantenimiento de servicios esenciales en sectores como la energía, el transporte o la sanidad. Para la identificación de las entidades críticas se tendrán en cuenta una serie de criterios que vienen establecidos en el art. 12 del anteproyecto. La Secretaría de Estado de Seguridad pondrá los elementos necesarios y pertinentes de la Evaluación Nacional de Amenazas y Riesgos a disposición de las entidades críticas que hayan sido identificadas, con el fin de garantizar que la información facilitada les ayude en la realización de sus evaluaciones de riesgos y en la adopción de medidas para garantizar su resiliencia. Por su parte, el art. 7 del anteproyecto establece que, sobre la base de la Estrategia y de los resultados de la Evaluación Nacional de Amenazas y Riesgos, la Secretaría de Estado de Seguridad elaborará, a través del Centro Nacional de Protección y Resiliencia de las Entidades Criticas (CNPREC, al cual se hará mención explícita *infra*), el Plan Nacional de Protección y Resiliencia de Entidades Críticas, que será el documento estructural que permitirá dirigir y coordinar las actuaciones precisas para fortalecer la seguridad de las entidades críticas y de sus infraestructuras, con el objetivo de garantizar la prestación de los servicios esenciales. Al mismo tiempo, el apdo. 2 de la mencionada disposición señala que la Secretaría de Estado de Seguridad elaborará un plan estratégico sectorial por cada uno de los sectores o subsectores de actividad recogidos en el anexo, adecuando al ámbito específico de cada sector los objetivos estratégicos y medidas de actuación previstos en la Estrategia, y teniendo en cuenta para ello los riesgos y amenazas de origen natural o humano que puedan dar lugar a un incidente, contenidos en la Evaluación Nacional de Amenazas y Riesgos e identificados específicamente para cada sector.

A partir de aquí, aquellas entidades incluidas en ese catálogo están obligadas no solo a llevar a cabo una evaluación de riesgos, sino también a elaborar y mantener actualizado un plan de resiliencia, el cual debe adecuarse a lo establecido en el art. 8. Dicho plan debe contemplar la identificación y evaluación de riesgos, así como la adopción de medidas técnicas, organizativas y de seguridad adecuadas para prevenir, proteger, responder y recuperarse ante incidentes que puedan afectar a la prestación de servicios esenciales. Según se establece en el art. 6, apdo. 2, del anteproyecto, la evaluación de riesgos tendrá en cuenta las amenazas derivadas de riesgos naturales y aquellas de origen humano que puedan dar lugar a un incidente. Entre las medidas concretas se incluyen la protección física de instalaciones, la gestión de la continuidad de las actividades, la formación y concienciación del personal, y la designación de un responsable de seguridad y resiliencia que actuará como punto de contacto con las autoridades competentes y como órgano responsable de seguridad y resiliencia de la entidad crítica a efectos del cumplimiento de las obligaciones previstas en el art. 8 del anteproyecto. Al mismo tiempo, el anteproyecto

también prevé en su art. 9 la implantación de un sistema de comprobación de antecedentes personales para garantizar la idoneidad de quienes prestan servicios en entidades críticas, así como la obligación de notificar cualquier incidente relevante que pueda alterar el funcionamiento de los servicios esenciales. No cabe duda de que ese sistema de comprobación de antecedentes personales supone tensionar en este contexto la seguridad de aquellas entidades que prestan servicios esenciales y un derecho fundamental como es la privacidad e intimidad de las personas que desarrollan distintas tareas en las mismas.

El art. 10 del anteproyecto se ocupa de la notificación de incidentes por parte de las entidades críticas, estableciéndose que estas deberán notificar a la Secretaría de Estado de Seguridad, a través del CNPREC, los incidentes que perturben o puedan perturbar de forma significativa la prestación de servicios esenciales en el plazo máximo de veinticuatro horas desde que tengan conocimiento de aquellos, salvo acreditada incapacidad, desde el punto de vista operativo, para hacerlo dentro de dicho plazo. Posteriormente, en un plazo no superior a un mes, presentarán un informe detallado del incidente. El propio precepto prevé que, cuando se considere que sea de interés general hacerlo, la Secretaría de Estado de Seguridad informará al público del incidente.

En cuanto al marco institucional y de gobernanza, el anteproyecto de mayo de 2025 establece que la Secretaría de Estado de Seguridad se configura como la autoridad nacional competente para la supervisión y cumplimiento de las disposiciones establecidas en la ley (art. 15). La misma actúa a través del Centro Nacional para la Protección y Resiliencia de las Entidades Críticas (CNPREC), organismo que sustituye al anterior Centro Nacional de Protección de Infraestructuras Críticas (CNPIC). Este centro será también el punto de contacto único para la cooperación transfronteriza con otros Estados miembros de la UE (art. 15, apdo. 2). Además, se crea la Comisión Nacional para la Protección y Resiliencia de las Entidades Críticas, órgano colegiado encargado de aprobar los planes estratégicos sectoriales y colaborar en la identificación de entidades críticas, así como un Grupo de Trabajo Interdepartamental para la coordinación de políticas en la materia. Tal y como señala el art. 19 del anteproyecto, dicho grupo de trabajo asistirá a la Secretaría de Estado de Seguridad en la elaboración de la Evaluación Nacional de Amenazas y Riesgos y de los planes estratégicos sectoriales.

Por último, el capítulo V (arts. 26-41) se ocupa de las tareas de supervisión de las entidades críticas, así como del régimen sancionador. Así, el art. 26 señala que las actividades de supervisión de las entidades críticas, dirigidas a evaluar el cumplimiento de las obligaciones establecidas en la ley, serán llevadas a cabo por la Secretaría de Estado de Seguridad. Para el desarrollo de estas actividades, la Secretaría de Estado de Seguridad tendrá, entre otras, las siguientes facultades (art. 26, apdo. 2): a) realizar inspecciones *in situ* de

las infraestructuras críticas y de las instalaciones que utilice la entidad crítica para prestar sus servicios esenciales; b) efectuar actividades de supervisión externa de las medidas adoptadas por las entidades críticas; c) realizar u ordenar auditorías.

Conviene señalar que, en relación con las entidades esenciales e importantes conforme a la ley por la que se transpone la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, que también hayan sido identificadas como críticas, la Secretaría de Estado de Seguridad estará facultada para requerir de la autoridad nacional designada conforme a la citada ley que, en el plazo que esta disponga, exija de aquellas que faciliten una serie de datos e informaciones que vienen especificados en el propio art. 26 del anteproyecto.

En lo que hace referencia al régimen sancionador, el art. 27 del anteproyecto establece que la responsabilidad por las infracciones previstas en la ley recaerá en las entidades críticas autoras del hecho en que consista la infracción. Ahora bien, sin perjuicio de esa responsabilidad corporativa, quienes ejerzan en la misma cargos de administración o dirección, sean unipersonales o colegiados, serán responsables de las infracciones cuando estas sean imputables a su conducta dolosa o negligente.

Al igual que se señaló al final del epígrafe anterior con respecto al anteproyecto de enero del año 2025, el aquí analizado anteproyecto dirigido a transponer la Directiva 2022/2557 contiene decisiones de interés, como la creación de una Estrategia Nacional para la Protección y Resiliencia de Entidades Críticas, así como la implantación del CNPREC. Es por ello por lo que sorprende que el actual Ejecutivo español no haya todavía avanzado en la gestación de un proyecto de ley que desemboque en la ley de transposición de la mencionada directiva. Y ello teniendo en cuenta las amenazas físicas a las que se encuentran actualmente expuestas entidades críticas ubicadas en el territorio de la UE. Para ello puede servir de ejemplo lo acontecido el pasado mes de enero en la red eléctrica de la capital alemana.

V. CONCLUSIONES

El pasado mes de marzo del año 2025, la actual presidenta de la Comisión Europea, Ursula von der Leyen, señaló que Europa debía prepararse para un eventual conflicto bélico[46]. Dichas declaraciones se enmarcan en una nueva

[46] Sobre esta cuestión, véase: «Von der Leyen quiere que los europeos estén preparados para la guerra», *ABC,* edición *online* de 22 de marzo de 2025. Disponible en: https://is.gd/8ufV0U.

Estrategia de Preparación de la Unión, elaborada por el Ejecutivo comunitario, y que será trasladada al Parlamento Europeo y a los Estados miembros (Comisión Europea, 2025).

En la mencionada estrategia, la Comisión Europea habla de múltiples riesgos y amenazas que al parecer se ciernen sobre la UE. Entre ellos se hace mención a potenciales episodios de «violencia armada». Al respecto, en las últimas fechas han aflorado informaciones procedentes de los servicios de inteligencia de varios Estados miembros que señalan que Rusia podría iniciar algún tipo de ataque contra algún país de la UE en los próximos diez años[47]. El Ejecutivo europeo también alerta sobre otros peligros como ataques híbridos o ciberataques contra infraestructuras europeas esenciales como redes de energía o bancos, sabotajes a cables submarinos, gasoductos y oleoductos, hasta grandes oleadas de desinformación por parte de potencias extranjeras con el objetivo de desestabilizar las democracias europeas. También se hace referencia a desastres naturales como incendios forestales, inundaciones o sequías. Para la Comisión, la amenaza que se cierne sobre la Europa comunitaria es de tal envergadura que incluso pide que todos los hogares europeos dispongan de reservas de agua, medicamentos, baterías y alimentos para subsistir 72 horas sin ayuda externa en caso de crisis.

No cabe duda de que el escenario descrito en los párrafos anteriores incide directamente en las infraestructuras y entidades críticas que proporcionan bienes y servicios esenciales a la población europea, y que han sido objeto de análisis —jurídico y criminológico— en la presente investigación publicada en dos partes. Por tanto, en estos momentos resulta primordial ajustar la protección física y cibernética de las infraestructuras y entidades críticas a las demandas procedentes sobre todo de la UE, para con ello incrementar la resiliencia de estas frente a amenazas naturales o cibernéticas, ya sean accidentales o causadas intencionadamente por el ser humano.

El pasado 7 de mayo de 2025, la Comisión Europea decidió enviar un dictamen motivado a diecinueve Estados miembros, entre los que se encontraban Alemania y España, por no haber notificado la plena transposición de la Directiva (UE) 2022/2555[48]. Como se sabe, los Estados miembros debían transponer dicha directiva al ordenamiento jurídico nacional a más tardar el

[47] Véase al respecto: «La UE teme que Putin ataque a un país de la OTAN antes de 2030: "Los servicios de inteligencia de Dinamarca y Alemania lo avisan"», *El Mundo,* edición *online* de 20 de marzo de 2025. Disponible en: https://is.gd/gx9vVx. Sobre la amenaza, a todos los niveles, procedente de Rusia, véase Marginedas (2025).

[48] Véase Comisión Europea, nota de prensa de 7 de mayo de 2025. Disponible en: https://is.gd/Uu4Psp.

17 de octubre de 2024. A partir de la notificación, dichos Estados disponían de dos meses para responder y adoptar las medidas necesarias. De no hacerlo, la Comisión podría optar por remitir los asuntos al Tribunal de Justicia de la Unión Europea.

Apenas dos meses más tarde, concretamente el 17 de julio de 2025, la misma Comisión decidió enviar sendos dictámenes motivados a trece países miembros de la UE, entre los que también se encuentran Alemania y España, por no haber notificado las medidas nacionales que transponen la Directiva relativa a la resiliencia de las entidades críticas (Directiva 2022/2557)[49]. También en este caso, los Estados miembros tenían que transponer esta directiva a más tardar el 17 de octubre de 2024. Notificados esos trece países por la Comisión, los mismos disponían de dos meses para responder y adoptar las medidas necesarias. De no hacerlo, la Comisión podría optar por remitir los asuntos al Tribunal de Justicia de la Unión Europea y solicitar que se les impongan sanciones financieras.

En estos momentos existen países de la UE que ya han logrado transponer a su derecho interno ambas directivas. Así, Bélgica implementó oficialmente la Directiva NIS-2 mediante la Ley del 26 de abril de 2024, así como un Real Decreto del 9 de junio de 2024, entrando finalmente en vigor el 18 de octubre de 2024. Dicha legislación es supervisada por el Centro de Ciberseguridad de Bélgica (CCB). Por lo que hace referencia a la Directiva CER, Bélgica se encuentra en las etapas finales de transposición, ya que el pasado 2 de diciembre de 2025 se aprobó en sede parlamentaria un proyecto de ley elaborado al efecto. Con respecto a Italia, en dicho país se ha completado también la transposición de la Directiva NIS-2 a través del Decreto Legislativo núm. 138, de 4 de septiembre de 2024, entrando en vigor el 16 de octubre de 2024. La Agenzia per la Cybersicurezza Nazionale (ACN) es la autoridad designada para llevar a cabo las tareas de supervisión. Italia también ha implementado la Directiva sobre Resiliencia de Entidades Críticas (Directiva CER) mediante el mismo decreto legislativo anteriormente referenciado.

Tal y como se ha podido comprobar en este trabajo, Alemania ha conseguido también transponer a su derecho interno las directivas NIS-2 y CER. Teniendo en cuenta las amenazas físicas y cibernéticas que se ciernen sobre el país germano, el actual Gobierno surgido de las elecciones celebradas el pasado año 2025 ha dado un impulso definitivo a los proyectos presentados en el año 2024, para con ello, entre otras cosas, evitar las correspondientes sanciones.

[49] Véase Comisión Europea, nota de prensa de 17 de julio de 2025. Disponible en: https://is.gd/ogjvvf.

Con los anteproyectos aprobados por el Gobierno español en enero y mayo del año 2025, el Ejecutivo pretende en primer lugar lograr la transposición definitiva de las directivas 2022/2555 y 2022/2557, implementado legislativamente medidas para lograr en elevado nivel de ciberseguridad en las entidades esenciales e importantes, así como reforzar la planificación, la coordinación institucional y la capacidad de respuesta por parte de las entidades críticas ante incidentes de origen físico que puedan comprometer la prestación de servicios esenciales, dotando a las mismas de obligaciones claras y mecanismos de apoyo y supervisión.

No obstante, conviene recordar que ambos textos aprobados por el Consejo de Ministros constituyen sendos anteproyectos, por lo que aún están sujetos a eventuales modificaciones durante su tramitación parlamentaria y en el proceso de consulta con los sectores y organismos implicados. El procedimiento de urgencia en su tramitación responde a la necesidad de transponer las mencionadas directivas 2022/2555 y 2022/2557 y de garantizar cuanto antes la seguridad, la resiliencia de los servicios esenciales en un contexto de amenazas crecientes y la interdependencia a escala europea[50]. Por ello, es de esperar que el actual Gobierno español convierta a la mayor brevedad ambos anteproyectos en proyectos de ley que desemboquen finalmente en su aprobación como leyes de transposición de derecho comunitario europeo, si bien la coyuntura política actual en España invita precisamente a todo lo contrario.

Bibliografía

Agustinoy, Albert y Sala, Mireia (2025). Futura Ley de protección y resiliencia de entidades críticas. *Cuatrecasas.* [blog], 2-6-2025. Disponible en: https://is.gd/LzJ59p.

Álvarez Fernández, César (2023). Directiva CER. Nuevo enfoque en la protección de las infraestructuras críticas. *Seguritecnia,* 17-2-2023. Disponible en: https://is.gd/XJLfL3.

Barrio Andrés, Moisés (2024). La ciberseguridad en el Derecho digital europeo: novedades de la Directiva NIS2. *InDret. Revista para el Análisis del Derecho,* 1, 504-531.

Beucher, Katharina; Ehlen, Thomas y Utzerath, Jan (2023). Kapitel 14. Kritische Infrastrukturen. En Denis-Kenji Kipker (ed.). *Cybersecurity* (pp. 502-578). Múnich: C. H. Beck.

Bundesamt für Sicherheit in der Informationstechnik. (s. f.). *Was sind Kritischen Infrastrukturen?* Disponible en: https://is.gd/lcYg4M.

[50] Véase al respecto Agustinoy y Sala (2025).

Bundesamt für Sicherheit in der Informationstechnik. Geschäftsstelle Up Kritis. (2014). *UP KRITIS Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen - Grundlagen und Ziele -.* Bonn: Geschäftsstelle UP KRITIS.

Bundesamt für die Sicherheit der nuklearen Entsorgung. (2020). *SEWD-Richlinie IT SKIII.* Disponible en: https://is.gd/YPIRn9.

Bundesministerium des Innern und für Heimat. (s. f.). *Schutz Kritischer Infrastrukturen.* Disponible: https://is.gd/m8Rzg1.

Bundesministerium des Innern und für Heimat. (2022). *Neuer Koordinierungsstab der Bundesregierung zum Schutz kritischer Infrastrukturen.* Nota de prensa, 21 de octubre de 2022. Disponible en: https://is.gd/qMqsWF.

Bundesministerium des Innern und für Heimat. (2022a). *Eckpunkte für das KRITIS-Dachgesetz.* Disponible en: https://is.gd/AiiXnH.

Cano Paños, Miguel Ángel (2025). Amenazas offline y online a infraestructuras críticas, con especial referencia a las centrales nucleares. Una visión político-criminal. *El Criminalista Digital. Papeles de Criminología,* 13, 93-104. Disponible en: https://is.gd/n3HRqk.

Canós Guillamón, Francisco Miguel (2025). Guía práctica de la Directiva NIS2. En José Wenceslao Ibáñez Jiménez (dir). *Tratado de Derecho de la Sociedad Digital* (vol. 2) (pp. 1363-1398). Madrid: Reus.

Comisión Europea. (2020). *Nueva Estrategia de Ciberseguridad de la UE y nuevas normas para aumentar la resiliencia de las entidades críticas físicas y digitales.* Comunicado de prensa, 16 de diciembre de 2020. Disponible en: https://is.gd/Ip1duv.

Comisión Europea. (2025). *Estrategia de Preparación de la Unión para prevenir amenazas y crisis emergentes y reaccionar frente a ellas.* Comunicado de prensa, 26 de marzo de 2025. Disponible en: https://is.gd/ZlPC7S.

Der Beauftragte der Bundesregierung für Informationstechnik. (s. f.). *Cybersicherheit in Kritischen Infrastrukturen.* Disponible en: https://is.gd/TjJYDu.

Gómez Castro, Juan Sebastián y Montilla Castilla, Martín (2025). Reglamento DORA: un cambio de paradigma en las obligaciones de ciberseguridad del sector financiero. *Actualidad Jurídica Uría Menéndez,* 67, 255-262. Disponible en: https://is.gd/9eTZGh.

González García, Julio (2025). Gestión de la ciberseguridad y la resiliencia digital en el sistema financiero: el Reglamento DORA. *Global Politics and Law,* 2-6-2025. Disponible en: https://is.gd/BDDqri.

Kipker, Dennis-Kenji (2024). Kritische Infrastruktur: Neuer Entwurf für Kritis-DachG. *Der Tagesspiegel,* 4-1-2024. Disponible en: https://is.gd/Emfk9r.

KPMG (2025). *Enhancing infrastructure resilience across Europe. An in-depth analisis of the new Critical Entities Resilience Directive (CER) and its impact in your organization.* Brussels: KPMG. Disponible en: https://is.gd/khhQ2J.

Lämmerhit, Philipp (2025). *Das NIS-2-Umsetzungsgesetz ist in Kraft getreten – welche Schritte sind nun erforderlich?* Datenschutz Notizen, 11-12-2025. Disponible en: https://is.gd/5BmP1o.

Marginedas, Marc (2025). *Rusia contra el mundo. Más de dos décadas de terrorismo de Estado, secuestros, mafia y propaganda.* Barcelona: Península.

Ministerio del Interior. (2025). *El Consejo de Ministros aprueba el anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.* Nota de prensa, 14 de enero de 2025. Disponible en: https://bit.ly/4u9wCJN.

Ministerio del Interior. (2025a). Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.

Ministerio del Interior. (2025b). Anteproyecto de Ley de Protección y Resiliencia de Entidades Críticas.

OpenKRITIS (2024). *NIS2 Umsetzungsgesetz.* Disponible en: https://is.gd/JupdLV.