BOLETÍN OFICIAL
DE LAS CORTES GENERALES

CONGRESO DE LOS DIPUTADOS

XV LEGISLATURA

Serie A:
PROYECTOS DE LEY **27 de marzo de 2026** **Núm. 88-1** **Pág. 1**

PROYECTO DE LEY

121/000088 Proyecto de Ley de protección y resiliencia de las entidades críticas.

La Mesa de la Cámara, en su reunión del día de hoy, ha adoptado el acuerdo que se indica respecto del asunto de referencia.

(121) Proyecto de ley.

Autor: Gobierno

Proyecto de Ley de protección y resiliencia de las entidades críticas.

Acuerdo:

Encomendar su aprobación con competencia legislativa plena, conforme al artículo 148 del Reglamento, a la Comisión de Interior. Asimismo, publicar en el Boletín Oficial de las Cortes Generales, estableciendo plazo de enmiendas, por un período de quince días hábiles, que finaliza el día 17 de abril de 2026.

En ejecución de dicho acuerdo se ordena la publicación de conformidad con el artículo 97 del Reglamento de la Cámara.

Palacio del Congreso de los Diputados, 24 de marzo de 2026.—P.D. El Secretario General del Congreso de los Diputados, **Fernando Galindo Elola-Olaso.**

cve: BOCG-15-A-88-1

PROYECTO DE LEY DE PROTECCIÓN Y RESILIENCIA DE LAS ENTIDADES CRÍTICAS

cve: BOCG-15-A-88-1

cve: BOCG-15-A-88-1

Exposición de motivos

I

La Constitución Española reconoce los derechos fundamentales y libertades públicas, que los poderes públicos deben garantizar. En el desarrollo de las medidas de protección que resulten adecuadas para garantizar estos derechos, se encuentran aquellas que permitan el funcionamiento efectivo de las entidades críticas, de forma que puedan prestar adecuadamente los servicios esenciales que demanda la ciudadanía.

Las entidades críticas son aquellas entidades u organismos, públicos o privados, proveedores de servicios esenciales y, en tal sentido, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, las considera como un ámbito de especial importancia para la seguridad nacional. 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 mercado interior, con una economía de la Unión Europea cada vez más interdependiente. La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, incorporó a nuestro ordenamiento interno 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 de mejorar su protección, y estableció un primer marco normativo de actuación con objeto de establecer las estrategias y las estructuras adecuadas que permitieran dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas. Sin embargo, esta norma se centraba exclusivamente en la protección de tales infraestructuras, desvinculada de la actividad de la entidad de la que formaban parte.

No obstante, la evaluación realizada en 2019 de la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, puso de manifiesto que, debido al carácter cada vez más interconectado y transfronterizo de las operaciones que utilizan infraestructuras críticas, las medidas de protección relativas únicamente a activos individuales no bastan para evitar que se produzcan perturbaciones. Por tanto, resultaba necesario modificar el enfoque para garantizar que se tuvieran mejor en cuenta los riesgos, se mejorase la definición y la coherencia de las funciones y las obligaciones de las entidades críticas que presten servicios esenciales para el funcionamiento del mercado interior de la Unión Europea, y se adaptasen sus normas a fin de aumentar la resiliencia de las entidades críticas de forma que éstas pudieran reforzar su capacidad de prevención, protección, respuesta, resistencia, mitigación, absorción, adaptación y recuperación ante incidentes que afecten a la prestación de servicios esenciales.

Con ese objetivo se aprobó la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, que, con efectos de 18 de octubre de 2024, es aplicable dentro del ámbito de la Unión. Esta 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. También se debe impulsar una mejora de su equipación, dada la existencia de un panorama dinámico de amenazas, entre las que figuran las amenazas híbridas y terroristas y las crecientes interdependencias entre estas infraestructuras y los sectores implicados. Además, debe tenerse en cuenta el aumento del riesgo físico derivado de las catástrofes naturales y del cambio climático, de modo que se han intensificado la frecuencia y la magnitud de los fenómenos meteorológicos extremos y los cambios a largo plazo en las condiciones climáticas medias que pueden mermar la capacidad, la eficiencia y la vida útil de determinados tipos de entidades e infraestructuras si no existen medidas de adaptación a dicho fenómeno.

El estado actual de estas entidades se caracteriza por la fragmentación en lo que respecta a la identificación y requisitos a cumplir por parte de las que se pueden

cve: BOCG-15-A-88-1

considerar críticas, pues existen sectores y categorías de entidades que no se reconocen sistemáticamente como críticos en todos los Estados miembros de la Unión Europea y, del mismo modo, la existencia de distintos grados de exigencia en las medidas de protección hacen que no sólo existan distintos niveles de resiliencia, sino que también pueda afectar negativamente al mantenimiento de sus funciones sociales o actividades económicas y se obstaculice su correcto funcionamiento. Por consiguiente, lo que se pretende conseguir a través de la Directiva UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, es un nivel sustancial de armonización en los sectores y categorías de estas entidades.

II

La resiliencia, entendida como la capacidad de las entidades para la prevención, la protección, la respuesta, la resistencia, la mitigación, la absorción, la adaptación y la recuperación de sus funciones en casos de incidente, resulta una cualidad para cuya consecución es necesario, en primer lugar, contar con una estrategia nacional en la que se establezcan los objetivos estratégicos para la mejora de la resiliencia de las entidades críticas, así como la adopción de un enfoque basado en el riesgo que se centre en las entidades más pertinentes para el desempeño de funciones sociales o actividades económicas vitales, cuyos resultados hagan posible tanto la identificación de las entidades que deban ser consideradas críticas, como el impulso de las actuaciones orientadas a la implementación de las medidas adecuadas para ayudar a éstas a alcanzar sus objetivos de resiliencia frente a los riesgos pertinentes. Al realizar la evaluación de riesgos es necesario, además, considerar las relaciones de interdependencia que pueden existir entre distintos sectores. Dentro de este contexto, es también esencial determinar las autoridades competentes para supervisar la aplicación y, en su caso, hacer cumplir las obligaciones derivadas de la aplicación de este marco normativo, como, por otra parte, lo es igualmente integrar adecuadamente estas actuaciones dentro de las políticas vigentes y de otras estrategias nacionales y sectoriales existentes en la materia, con la premisa de alcanzar un enfoque global.

En este sentido, dada la importancia de la ciberseguridad para la resiliencia de las entidades críticas, en aras de la coherencia y de la evitación de cargas administrativas excesivas, debe garantizarse, siempre que sea posible, un enfoque coherente entre la normativa aplicable en virtud de la Directiva (UE) 2022/2557 de 14 de diciembre, y la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Teniendo en cuenta la mayor frecuencia y las características particulares de los riesgos cibernéticos, se debe tener en consideración que la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, impone unos requisitos exhaustivos a un amplio conjunto de entidades para garantizar su ciberseguridad.

Por ello, puesto que la ciberseguridad se encuentra suficientemente tratada en dicha norma comunitaria, las materias reguladas por la misma deben quedar excluidas del ámbito de aplicación de esta ley, sin perjuicio de determinadas peculiaridades contenidas en ella relativas a las entidades del sector de las infraestructuras digitales que puedan ser, asimismo, consideradas infraestructuras críticas. No obstante, a fin de alcanzar un enfoque global, se debe garantizar el establecimiento de un marco de actuación para mejorar la coordinación entre las autoridades competentes con arreglo a esta ley y las autoridades competentes con arreglo a la norma que transponga la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, 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. En la puesta en

cve: BOCG-15-A-88-1

marcha de estas estrategias, se debe tener en cuenta, además, la naturaleza híbrida de las amenazas para las entidades críticas.

Asimismo, a fin de evitar duplicidades y cargas innecesarias, las disposiciones de esta ley no deben aplicarse si las disposiciones sectoriales obligan a las entidades críticas a adoptar medidas para aumentar su resiliencia que sean reconocidas como, al menos, equivalentes a las establecidas en esta norma. Tampoco afectan a las competencias públicas relativas al mantenimiento de la seguridad nacional y la defensa, o para salvaguardar otras funciones esenciales del Estado, en particular, por lo que atañe a la seguridad pública, la integridad territorial y el mantenimiento del orden público.

III

Esta ley consta de cuarenta y un artículos, estructurados en cinco capítulos, así como de nueve disposiciones adicionales, una transitoria, una derogatoria y siete finales.

En el capítulo I se regula el objeto y el ámbito de aplicación objetivo y subjetivo. Se incluyen las principales definiciones, de forma que todos los agentes implicados en su aplicación tengan conocimiento de los elementos básicos para encontrar el sentido y alcance de cada precepto.

El capítulo II establece el marco nacional para la resiliencia de las entidades críticas, en el que se define el entorno legal para la planificación y evaluación de la protección y resiliencia de las entidades críticas de manera que se garanticen los mayores estándares en las medidas y medios técnicos y organizativos de protección. Es relevante señalar que para ello se desarrolla una Estrategia Nacional de Protección y Resiliencia de las Entidades Críticas de forma que se obtenga un enfoque global de esta cualidad por parte de las entidades críticas para que, sobre la base de una Evaluación Nacional de las Amenazas y Riesgos a los que se encuentran sometidas las entidades, las citadas medidas se adapten al nivel resultante del análisis y sean eficientes, eficaces y se obligue a su implantación efectiva, más allá de posibles aplicaciones nominales de las medidas a adoptar.

Otras medidas para potenciar la resiliencia de las entidades críticas consisten en la realización de una evaluación individualizada del riesgo por parte de las distintas entidades, y detallar las actuaciones singulares a llevar a cabo por estas, para garantizar y elevar sus niveles de resiliencia mediante la adopción de medidas eficientes, eficaces y adecuadas al resultado de su análisis de riesgos, que deben quedar encuadradas en un plan de resiliencia específico. También se establece un sistema de comprobación de identidad de las personas que desempeñen determinados cometidos o deban acceder a instalaciones, información o sistemas de control de éstas y determina las obligaciones de notificación de incidentes.

La creación de un esquema nacional de certificación en materia de resiliencia de las entidades críticas constituye una novedad en esta norma. Esto permitirá a las entidades garantizar que sus medidas se acomodan a un esquema de certificación que analice los aspectos globales de su operativa, estandarizando y mostrando los niveles de calidad, seguridad y cumplimiento.

En este capítulo se incluye, igualmente, el sistema para la identificación de las entidades críticas, introduciéndose el concepto de efecto perturbador significativo, así como las particularidades de las entidades que pertenecen al sector bancario, de las infraestructuras de los mercados financieros y de las infraestructuras digitales. El asesoramiento a las entidades se convierte en una de las piedras angulares del sistema de protección y resiliencia a implementar.

Resulta relevante la creación de un Catálogo Nacional de Entidades Críticas y Estratégicas, que integra la información relativa a las infraestructuras críticas, preservando el carácter clasificado de estas últimas, de forma que se contenga la información de las entidades críticas que permita a las autoridades competentes cumplir con sus misiones y, de forma singularizada, específica y con la necesaria protección, la información sobre las concretas infraestructuras criticas pertenecientes a las distintas

cve: BOCG-15-A-88-1

entidades. De esta forma, se facilita el cumplimiento de esta ley por parte de todos los agentes implicados y se mantiene el sistema de protección de la información relativa a elementos concretos que, por su importancia, sólo deben ser conocidos por un reducido número de personas.

En el capítulo III se regula el marco institucional para la protección y resiliencia de las entidades críticas, en el que se detallan las instituciones y órganos a través de los cuales se asumen las distintas responsabilidades en la aplicación del marco normativo para la protección y resiliencia de aquellas.

El capítulo IV aborda las entidades críticas de especial importancia europea, entendidas como aquellas entidades identificadas como críticas que, además, prestan los mismos o similares servicios esenciales a o en seis o más Estados miembros de la Unión Europea. Esta figura está concebida como un mecanismo para responder a la existencia real de una red cada vez más interconectada de prestación de servicios e infraestructuras que proporcionan servicios esenciales en más de un Estado miembro, garantizando en todos ellos un nivel homogéneo en las medidas destinadas a asegurar un elevado nivel de resiliencia. A tal fin, se prevé la posibilidad de organizar, por parte de la Comisión Europea, con participación de representantes de los Estados a o en los que se prestan dichos servicios, misiones de asesoramiento para evaluar las medidas adoptadas por estas entidades críticas de especial importancia europea.

El capítulo V, relativo al régimen sancionador, regula el ejercicio de competencias de supervisión para evaluar el cumplimiento de las obligaciones establecidas en esta ley, junto con el establecimiento del deber legal de colaboración por parte de las entidades críticas supervisadas, y la concreción de un marco específico de colaboración en este ámbito con las autoridades competentes en relación con las infraestructuras digitales.

La Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre, dispone que los Estados establecerán el régimen de sanciones aplicables a cualquier incumplimiento de las normas adoptadas al amparo de su contenido y aprobarán las medidas necesarias para garantizar su ejecución, exigiéndose que el sistema de sanciones que se implemente sea efectivo, proporcionado y disuasorio. A tal fin, este capítulo incorpora las previsiones necesarias para el cumplimiento de lo expuesto, estableciéndose un sistema que, además de cumplir con las previsiones de la normativa de la Unión Europea, garantice, conforme a nuestro ordenamiento jurídico, todos los derechos de las personas interesadas.

La parte final de la ley incorpora nueve disposiciones adicionales, entre las que puede destacarse la referencia al tratamiento denominado «Informes y comprobaciones para acreditaciones y antecedentes», destinado a posibilitar la realización de las comprobaciones necesarias en relación con la prevención de ilícitos penales y amenazas graves contra la seguridad pública en instalaciones y entidades críticas, entre otros ámbitos, emitiendo acreditaciones o informes de idoneidad, dando con ello respaldo al cumplimiento de la exigencia, prevista en la Directiva (UE) 2022/2557, del establecimiento de un procedimiento de comprobación de antecedentes personales. Traslada a la norma las obligaciones de comunicación a la Comisión de los distintos hitos relacionados con la implementación de las disposiciones de la Directiva.

Por medio de la disposición derogatoria se deroga la Ley 8/2011, de 28 de abril, y cuantas disposiciones de igual o inferior rango se opongan a esta ley.

Por último, en las disposiciones finales se lleva a cabo una modificación puntual del texto refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por el Real Decreto Legislativo 2/2011, de 5 de septiembre, para adecuarla a esta norma; se recoge el título competencial habilitante; se salvaguarda la información en el ámbito de la seguridad nacional, la seguridad pública o la defensa nacional; se salvaguardan asimismo las competencias autonómicas en materia de protección civil; se señala que por medio de esta norma se incorpora al Derecho español la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022; se procede a habilitar al Gobierno para dictar el desarrollo reglamentario de esta norma; y se establece su entrada en vigor. En cuanto al desarrollo reglamentario, cabe destacar la

cve: BOCG-15-A-88-1

previsión contenida en la disposición final sexta, relativa a la modificación mediante orden ministerial de la relación de sectores, subsectores y entidades recogidos en el anexo de la Ley, a fin de posibilitar progresivamente la incorporación de sectores adicionales o la cobertura de nuevas necesidades, como puede ser el caso de sectores tan significativos como la protección social, previa evaluación del cumplimiento de los requisitos previstos en el artículo 2 y concordantes de la Ley.

IV

En la elaboración de esta ley se han observado los principios de buena regulación exigidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En primer lugar, se trata de una norma necesaria, dado que la transposición de la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, exige el desarrollo de una norma de rango legal, cumpliéndose con el principio de eficacia al identificarse de manera clara los fines que persigue, a saber, garantizar la protección y resiliencia de las entidades críticas, y es el instrumento más adecuado para garantizar su consecución.

Se garantiza el principio de seguridad jurídica, por cuanto la norma es coherente con el resto del ordenamiento jurídico, nacional y de la Unión Europea, y genera un marco normativo estable, predecible, integrado, claro y de certidumbre, que facilita su conocimiento y comprensión y, en consecuencia, la actuación y toma de decisiones por los destinatarios de la norma.

Respecto al principio de proporcionalidad, esta ley contempla las garantías necesarias para que las posibles afectaciones a los derechos que pudieran verse implicados y las obligaciones dirigidas a las entidades y personas afectadas resulten proporcionales, oportunas, mínimas y suficientes, a fin de cumplir con los objetivos que se persiguen, es decir, garantizar la prestación sin obstrucciones en el mercado interior de servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales, identificar a las entidades críticas, apoyarlas en el cumplimiento de las obligaciones establecidas, muy en concreto las relativas a las implementadas para que se aumente su resiliencia y capacidad de prestar los servicios aludidos y garantizar la supervisión de la norma, lo que incluye el desarrollo de un régimen sancionador.

En cuanto al principio de eficiencia, la norma no impone cargas administrativas innecesarias o accesorias y racionaliza, en su aplicación, la gestión de los recursos públicos.

Se cumple, también, con el principio de transparencia, puesto que esta ley ha sido sometida a los correspondientes trámites de participación ciudadana, esto es, el de consulta pública y el de audiencia e información pública.

En su tramitación, además de los diversos Ministerios concernidos por razón de la materia, ha emitido informe la Agencia Española de Protección de Datos. Asimismo, ha sido objeto de dictamen por parte del Consejo de Estado.

Por último, la ley se dicta al amparo de la regla 29.ª del artículo 149.1 de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Esta ley tiene por objeto:

a) Definir e identificar las entidades críticas y establecer medidas específicas destinadas a garantizar la prestación sin obstrucciones de los servicios esenciales para

cve: BOCG-15-A-88-1

el mantenimiento de las funciones sociales o las actividades económicas vitales por parte de aquellas.

b) Establecer obligaciones para la mejora de la resiliencia de las entidades críticas, a fin de garantizar la capacidad de prestación y mantenimiento de los correspondientes servicios esenciales.

c) Implantar procedimientos comunes de cooperación e información, y medidas para garantizar la supervisión del cumplimiento y ejecución de las obligaciones por parte de las entidades críticas.

Artículo 2. *Definiciones.*

A los efectos de esta ley se entiende por:

a) Criterios de efectos perturbadores significativos: los parámetros mediante los cuales se puede determinar el impacto sobre la prestación de servicios esenciales.

b) Criterios horizontales de criticidad: parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica. Se evaluarán en función de:

1.º El número de personas afectadas, valorado en atención al número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública, así como para colectivos especialmente vulnerables.

2.º El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.

3.º El impacto medioambiental, degradación en el lugar y sus alrededores.

4.º El impacto público y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

c) Entidad crítica: entidad u organismo, público o privado, identificado conforme a lo previsto en el artículo 12 como perteneciente a una de las categorías de entidades recogidas en el anexo.

d) Entidad crítica de especial importancia europea: 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.

e) Entidad estratégica: entidad u organismo, público o privado, responsable del funcionamiento o gestor de una infraestructura catalogada como estratégica con arreglo a esta ley.

f) Especificación técnica: documento en el que se prescriben los requisitos técnicos que debe reunir un producto, proceso, servicio o sistema y que establece uno o más de los aspectos siguientes:

1.º Las características que debe tener un producto, como los niveles de calidad, rendimiento, interoperabilidad, protección del medio ambiente, salud y seguridad y sus dimensiones, así como los requisitos aplicables al producto en lo que respecta a la denominación con la que se vende, la terminología, los símbolos, los ensayos y los métodos de ensayo, el embalaje, el marcado o el etiquetado y los procedimientos de evaluación de la conformidad.

2.º Los métodos y procedimientos de producción de los productos agrícolas, definidos en el artículo 38, apartado 1, del TFUE, de los productos destinados a la alimentación humana y animal y de los medicamentos, así como los métodos y procedimientos de producción relacionados con los demás productos, en caso de que estos influyan en sus características.

3.º Las características que debe tener un servicio, como los niveles de calidad, rendimiento, interoperabilidad, protección del medio ambiente, salud o seguridad, así como los requisitos aplicables al proveedor en lo que respecta a la información que debe

cve: BOCG-15-A-88-1

facilitarse al destinatario, tal como se especifica en el artículo 22, apartados 1 a 3, de la Directiva 2006/123/CE.

4.º Los métodos y los criterios para evaluar el rendimiento de los productos de construcción, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) no 305/2011 del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, por el que se establecen condiciones armonizadas para la comercialización de productos de construcción, y se deroga la Directiva 89/106/CEE;

g) Evaluación de riesgos: el proceso general dirigido a determinar la naturaleza y el alcance de un riesgo, mediante la identificación y el análisis de potenciales amenazas, vulnerabilidades y peligros pertinentes que puedan dar lugar a un incidente y mediante la evaluación de las posibles pérdidas o perturbaciones en la prestación de un servicio esencial causadas por dicho incidente.

h) Incidente: un acontecimiento que tiene el potencial de perturbar significativamente o que perturba la prestación de un servicio esencial, en particular cuando afecte a los sistemas nacionales que salvaguardan el Estado de Derecho.

i) Infraestructura crítica: 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 y en la que concurre alguno de los criterios horizontales de criticidad.

j) Infraestructura estratégica: un elemento, instalación, equipo, red o sistema, o parte de un elemento, instalación, equipo, red o sistema, que, sin ser crítico, es relevante para la prestación de un servicio esencial.

k) Interdependencias: los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, autonómico, nacional o internacional.

l) Norma: especificación técnica adoptada por un organismo de normalización reconocido, de aplicación repetida o continua, cuya observancia no es obligatoria, y que reviste una de las formas siguientes: norma internacional, norma europea, norma armonizada o norma nacional.

m) Resiliencia: la capacidad de una entidad crítica para la prevención, la protección, la respuesta, la resistencia, la mitigación, la absorción, la adaptación y la recuperación en caso de un incidente.

n) Riesgo: la posible pérdida o perturbación causada por un incidente expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal incidente.

ñ) Sector estratégico: cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo.

o) Servicio esencial: servicio que es crucial para el mantenimiento de las funciones sociales vitales, de las actividades económicas, de la salud pública, de la seguridad o del medio ambiente.

p) Subsector estratégico: cada una de las subáreas en las que se dividen los distintos sectores estratégicos, conforme a la distribución contenida en el anexo.

Artículo 3. *Ámbito de aplicación.*

1. Esta ley es aplicable a las entidades críticas que operen en el territorio nacional, vinculadas a los sectores y subsectores estratégicos definidos en el anexo.

2. Quedan fuera de su ámbito de su aplicación:

a) Las entidades críticas dependientes del Ministerio de Defensa, de las Fuerzas y Cuerpos de Seguridad del Estado y de los cuerpos de policía de las Comunidades Autónomas con competencias estatutarias para la protección de personas y bienes y

cve: BOCG-15-A-88-1

para el mantenimiento del orden público, que se regirán, a efectos de control administrativo, por su propia normativa y procedimientos.

b) Las materias reguladas en la ley por la que se transponga la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148, sin perjuicio de lo previsto en la disposición adicional cuarta**.**

c) El Banco de España.

3. Asimismo, las disposiciones de esta ley no serán de aplicación cuando otras normas sectoriales obliguen a las entidades críticas a adoptar medidas para aumentar su resiliencia, siempre que tales obligaciones sean reconocidas en esas normas o, en su defecto, en una resolución de la persona titular del Ministerio del Interior, a propuesta de la Secretaría de Estado de Seguridad como equivalentes a las establecidas en esta ley.

4. La aplicación de esta ley se efectuará sin perjuicio de otros regímenes legales destinados a garantizar la prestación de los servicios esenciales en sectores concretos, como:

a) La seguridad nacional, la defensa y las competencias para preservar otras funciones esenciales del Estado, garantizando la integridad territorial, manteniendo la seguridad pública y la gestión de los procesos electorales y consultas directas al electorado.

b) La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

c) La Ley 25/1964, de 29 de abril, sobre energía nuclear (y sus normas de desarrollo), y la Ley 15/1980, de 22 de abril, de creación del Consejo de Seguridad Nuclear.

d) La Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil, y sus normas de desarrollo, así como la normativa autonómica en la materia.

e) El Programa Nacional de Seguridad de la Aviación Civil de la Ley 21/2003, de 7 de julio, de Seguridad Aérea, y sus normas de desarrollo.

f) El Real Decreto 1617/2007, de 7 de diciembre, por el que se establecen medidas para la mejora de la protección de los puertos y del transporte marítimo.

g) La Ley 24/2013, de 26 de diciembre, del sector eléctrico, y la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos, y sus respectivas normas de desarrollo.

h) La Ley 19/2003, de 4 de julio, sobre régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior y sobre determinadas medidas de prevención del blanqueo de capitales, y, en concreto, a su artículo 7bis relativo a la suspensión del régimen de liberalización de determinadas inversiones extranjeras directas en España.

CAPÍTULO II

Marco nacional para la resiliencia de las entidades críticas

Sección 1.ª Instrumentos y planes para la protección y resiliencia de las entidades críticas

Artículo. 4. *Estrategia Nacional de Protección y Resiliencia de las Entidades Críticas.*

1. El Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, a propuesta de la persona titular del Ministerio del Interior, tras consultar a las partes interesadas, aprobará la Estrategia Nacional de Protección y Resiliencia de las Entidades Críticas (en adelante, la Estrategia), relativa a los sectores y subsectores indicados en el anexo. La Estrategia será elaborada por la Secretaría de Estado de Seguridad, como autoridad nacional competente de acuerdo con el artículo 15, con el apoyo del Comité Interdepartamental para la Protección y Resiliencia de las Entidades Críticas.

cve: BOCG-15-A-88-1

2. La 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 y abarcará, como mínimo, los siguientes elementos respecto de los sectores indicados en el anexo:

a) Los objetivos estratégicos y las prioridades con el fin de aumentar la resiliencia global de las entidades críticas, teniendo en cuenta las dependencias e interdependencias transfronterizas e intersectoriales.

b) Un marco de gobernanza para alcanzar los objetivos estratégicos y las prioridades, incluida una descripción de las funciones y responsabilidades de las diferentes autoridades, de las entidades críticas y de otras partes implicadas en la aplicación de la estrategia.

c) Una descripción de las medidas necesarias para aumentar la resiliencia global de las entidades críticas, incluida una descripción de la Evaluación Nacional de Amenazas y Riesgos.

d) Una descripción del proceso por el que se identifican las entidades críticas.

e) Una descripción del proceso de apoyo a las entidades críticas, incluidas las medidas para mejorar la cooperación entre el sector público, por una parte, y el sector privado y las entidades públicas y privadas, por otra.

f) Una lista de las principales autoridades y partes interesadas pertinentes, distintas de las entidades críticas, que participen en la ejecución de la Estrategia.

g) Un marco de actuación para la coordinación con las autoridades competentes con arreglo a la ley por la que se transponga la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, a efectos 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 con el ejercicio de las tareas de supervisión y al Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011.

h) Una descripción de las medidas adoptadas con el fin de facilitar el cumplimiento de las obligaciones en materia de resiliencia establecidas en el capítulo IV por parte de las identificadas como entidades críticas.

3. La Estrategia se actualizará, como mínimo, cada cuatro años, o siempre que se produzca un cambio sustancial en las circunstancias a valorar, tras consultar a las partes interesadas dando cuenta a la Comisión en el plazo de los tres meses siguientes a su adopción o actualización.

Artículo 5. *Evaluación Nacional de Amenazas y Riesgos.*

1. La Secretaría de Estado de Seguridad procederá a la elaboración y aprobación de una Evaluación Nacional de Amenazas y Riesgos sobre, al menos, la lista no exhaustiva de servicios esenciales establecida en el Reglamento Delegado (UE) 2023/2450 de la Comisión, de 25 de julio de 2023, por el que se completa la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, estableciendo una lista de servicios esenciales, adaptada a las especificidades nacionales.

2. 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, dando cuenta a la Comisión en el plazo de los tres meses siguientes a su adopción o actualización.

3. La elaboración de la Evaluación Nacional de Amenazas y Riesgos tendrá en cuenta los riesgos o amenazas de origen natural o humano pertinentes que puedan dar

cve: BOCG-15-A-88-1

lugar a un incidente, incluidos los de naturaleza intersectorial o transfronteriza, los accidentes, las catástrofes naturales, las emergencias de salud pública y las amenazas híbridas u otras amenazas antagónicas, incluida la amenaza terrorista.

4. Al realizar la evaluación de riesgos se analizará, como mínimo, lo siguiente:

a) La evaluación general de riesgos realizada de conformidad con el artículo 6.1 de la Decisión 1313/2013/UE del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, relativa a un Mecanismo de Protección Civil de la Unión.

b) Otras evaluaciones de riesgos pertinentes realizadas de conformidad con:

1.º El Reglamento (UE) 2017/1938 del Parlamento Europeo y del Consejo, de 25 de octubre de 2017, sobre medidas para garantizar la seguridad del suministro de gas y por el que se deroga el Reglamento (UE) n.º 994/2010.

2.º El Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre la preparación frente a los riesgos en el sector de la electricidad y por el que se deroga la Directiva 2005/89/CE.

3.º El Real Decreto 903/2010, de 9 de julio, de evaluación y gestión de riesgos de inundación.

4.º El Real Decreto 840/2015, de 21 de septiembre, por el que se aprueban medidas de control de los riesgos inherentes a los accidentes graves en los que intervengan sustancias peligrosas.

5.º La Ley 7/2021, de 20 de mayo, de cambio climático y transición energética.

c) Los riesgos pertinentes derivados del grado de interdependencia de los sectores indicados en el anexo, incluido el grado en que dependen de entidades situadas en otros Estados miembros y en terceros países, y las repercusiones que una perturbación significativa en un sector pueda tener en otros sectores, incluido cualquier riesgo significativo para los ciudadanos y el mercado interior.

d) Cualquier información sobre incidentes notificados que perturben o puedan perturbar de forma significativa la prestación de los servicios esenciales.

5. La Secretaría de Estado de Seguridad, a través del punto de contacto único, 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 las ayude en la realización de sus evaluaciones de riesgos y en la adopción de medidas para garantizar su resiliencia.

Artículo 6. *Evaluación de riesgos por parte de las entidades críticas.*

1. Las entidades críticas deberán realizar una evaluación de riesgos que, sobre la base de la Evaluación Nacional de Amenazas y Riesgos y otras fuentes de información, determine el nivel de riesgo de la materialización de las amenazas que puedan perturbar la prestación de los servicios esenciales. En el plazo máximo de nueve meses posteriores a la notificación de su identificación como entidad crítica, esta elevará su evaluación de riesgos a la Secretaría de Estado de Seguridad para su validación. Asimismo, siempre que sea necesario y, en todo caso, cada cuatro años, las entidades críticas deberán realizar una nueva evaluación de riesgos.

2. La evaluación de riesgos tendrá en cuenta las amenazas derivadas de riesgos naturales, riesgos técnicos y las de origen humano que puedan dar lugar a un incidente, entre ellas, las de naturaleza intersectorial o transfronteriza, los accidentes, las catástrofes naturales, las emergencias de salud pública, las amenazas híbridas y otras amenazas antagónicas, incluidos los delitos de terrorismo y crimen organizado. Asimismo, tendrá en cuenta el grado de interdependencia entre el servicio esencial prestado por dicha entidad crítica y otros sectores indicados en el anexo, así como con otros servicios esenciales prestados por otras entidades en esos sectores, y también, cuando proceda, con Estados miembros vecinos y con terceros países.

cve: BOCG-15-A-88-1

3. Cuando se hayan realizado otras evaluaciones o análisis de riesgos o elaborado documentos en virtud de obligaciones establecidas en otras normativas o instrumentos jurídicos que sean pertinentes para su evaluación de riesgos, la entidad crítica podrá utilizar esas otras evaluaciones y documentos para cumplir con los requisitos establecidos en este artículo. En el ejercicio de sus funciones de validación, la Secretaría de Estado de Seguridad podrá declarar conforme, total o parcialmente, con estas obligaciones una evaluación de riesgos existente realizada de acuerdo con lo dispuesto en este apartado

Artículo 7. *Sistema de planificación para la protección y resiliencia de las entidades críticas.*

1. 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 y aprobará, 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.

2. Asimismo, la Secretaría de Estado de Seguridad, a través del Centro Nacional para la Protección y Resiliencia de las Entidades Críticas (en adelante, CNPREC), 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 teniendo en cuenta 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.

Los planes estratégicos sectoriales, que serán aprobados por la Comisión Nacional, podrán tener en cuenta otros planes o programas ya existentes, creados sobre la base de su propia legislación específica sectorial. Cuando los referidos planes o programas sectoriales reúnan los requisitos necesarios para identificar y dar respuesta a las vulnerabilidades y amenazas potenciales de un sector concreto, con un resultado equivalente al previsto en el párrafo anterior, la Secretaría de Estado de Seguridad podrá adoptarlos como plan estratégico sectorial del sector o subsector correspondiente.

3. Los Planes de Resiliencia de las entidades críticas serán elaborados por cada una de las entidades identificadas como tales, y se adecuarán a lo establecido en el artículo 8.

4. Los Planes de Apoyo Operativo serán elaborados por las Fuerzas y Cuerpos de Seguridad en relación con cada una de las infraestructuras críticas existentes en su demarcación territorial de competencia, operadas por las distintas entidades críticas, para lo que contarán con la colaboración del delegado de seguridad de la infraestructura crítica previsto en el artículo siguiente. En ellos se deberán contemplar medidas de vigilancia, prevención o reacción complementarias a las previstas por la entidad crítica en su plan de resiliencia para cada una de sus infraestructuras críticas, así como, en su caso, la coordinación con otros órganos de la Administración u organismos públicos competentes, en atención a sus respectivos ámbitos competenciales.

5. El contenido y procedimiento de elaboración, aprobación y registro de cada uno de los planes se determinarán reglamentariamente.

Artículo 8. *Plan de Resiliencia.*

1. Las entidades críticas deben adoptar un Plan de Resiliencia que contenga las medidas técnicas, organizativas, procedimentales u operativas de seguridad adecuadas y proporcionadas para garantizar su resiliencia, en el marco del plan estratégico sectorial correspondiente, y sobre la base de la información pertinente de la Evaluación Nacional de Amenazas y Riesgos prevista en el artículo 5 y de los resultados de la Evaluación de

cve: BOCG-15-A-88-1

riesgos de la entidad crítica regulada en el artículo 6. Dicho plan incluirá las medidas necesarias para:

a) Evitar que se produzcan incidentes, valorando especialmente medidas de reducción del riesgo de catástrofes y de adaptación al cambio climático.

b) Garantizar una protección física adecuada de sus instalaciones y de la infraestructura crítica, en especial, las vallas, las barreras, las herramientas y rutinas de vigilancia perimetral, los equipos de detección y los controles de acceso, entre otros.

c) Responder y resistir a las consecuencias de los incidentes y mitigarlas, considerando especialmente la aplicación de procedimientos y protocolos de gestión de riesgos y crisis y rutinas de alerta.

d) Recuperarse de incidentes, atendiendo en especial a medidas de continuidad de las actividades y la identificación de cadenas de suministro alternativas, a fin de retomar la prestación del servicio esencial.

e) Garantizar una gestión adecuada de la protección de los empleados, valorando específicamente medidas tales como la determinación de las categorías del personal que ejerce funciones esenciales, el establecimiento de derechos de acceso a instalaciones, infraestructuras críticas e información delicada, el establecimiento de procedimientos de comprobación de idoneidad de las personas de conformidad con el artículo 9 e identificando expresamente y de forma motivada, para cada infraestructura crítica y activo crítico de la entidad, las categorías de puestos o funciones cuyo desempeño justifica la realización de dichas comprobaciones y el nivel de comprobación aplicable, y la designación de las categorías de personas obligadas a someterse a la misma, así como el establecimiento de requisitos adecuados en materia de formación y cualificaciones. A los efectos de este párrafo, se tendrá en cuenta al personal de los proveedores de servicios externos a la hora de establecer categorías de personal que ejerza funciones esenciales.

f) Concienciar al personal acerca de las medidas mencionadas en los párrafos anteriores, considerando especialmente medidas como la organización de cursos de formación y ejercicios y la elaboración de material de información.

g) Realizar simulacros de distintas amenazas con la colaboración de los cuerpos policiales competentes territorial y funcionalmente.

En el plazo máximo de los seis meses posteriores a la realización de la evaluación de riesgos de la entidad crítica, o de su renovación, ésta deberá elaborar su Plan de Resiliencia y remitirlo, para su validación, a la Secretaría de Estado de Seguridad, que deberá prestar especial atención a que los puestos para los que se prevé la posibilidad de comprobaciones de idoneidad estén suficientemente motivadas y justificadas, rechazándolas en caso contrario.

2. Las entidades críticas podrán utilizar el plan de resiliencia o documento equivalente para cumplir con los requisitos establecidos en este artículo. En el ejercicio de sus funciones de validación, la Secretaría de Estado de Seguridad podrá declarar conforme con estas obligaciones, total o parcialmente, las medidas existentes de mejora de la resiliencia tomadas por una entidad crítica que aborden, de forma adecuada y proporcionada, las medidas técnicas, organizativas, procedimentales u operativas de seguridad a que se refiere el apartado 1.

3. En el plazo de los tres meses posteriores a su designación como tales, las entidades críticas nombrarán y comunicarán a la Secretaria de Estado de Seguridad a través del CNPREC la designación de una persona, unidad u órgano como responsable de seguridad y resiliencia de la entidad crítica a efectos del cumplimiento de las obligaciones previstas en este artículo, y como punto de contacto con las autoridades competentes. Las posteriores renovaciones del puesto de responsable de seguridad y resiliencia se comunicarán en el plazo de 72 horas. Esta persona, o el titular de la citada unidad u órgano, deberán contar con la habilitación de Director de Seguridad expedida

cve: BOCG-15-A-88-1

por el Ministerio del Interior, en los términos previstos en la normativa de seguridad privada.

Cada infraestructura crítica contará con un delegado de seguridad, designado por la entidad crítica como punto de contacto con el cuerpo policial competente para la elaboración del correspondiente Plan de Apoyo Operativo. Su designación o renovación se comunicarán en los mismos términos señalados en el párrafo anterior.

Asimismo, las entidades críticas dispondrán de un Área de Seguridad con las características y funciones que se determinen reglamentariamente. La persona responsable de seguridad y resiliencia podrá ostentar la jefatura de esta área.

Sección 2.ª Otras medidas de protección y resiliencia de las entidades críticas

Artículo 9. *Comprobación de idoneidad de las personas.*

1. Teniendo en cuenta el nivel de amenazas y riesgos notificado a las entidades críticas en virtud de la Evaluación Nacional de Amenazas, estas podrán presentar, de forma motivada, solicitudes de comprobación de idoneidad a la Secretaría de Estado de Seguridad, conforme a lo dispuesto en el artículo 8, en relación con las infraestructuras críticas y activos críticos expresamente determinados en el mismo, y que:

a) Desempeñen tareas sensibles en la entidad crítica o para su beneficio directamente relacionadas con la resiliencia de la entidad crítica.

b) Desempeñen funciones directamente vinculadas a la operación, mantenimiento, protección o control de las infraestructuras críticas o activos críticos de la entidad.

c) Estén siendo considerados para su contratación en puestos que cumplan los criterios establecidos en los dos párrafos anteriores, siempre que dichos puestos estén específicamente identificados en el Plan de Resiliencia como sujetos a comprobación previa.

2. En el ámbito de aplicación de esta ley se define la evaluación de la idoneidad como la comprobación de la identidad de una persona, incluidos los antecedentes penales, como parte de las medidas que debe implementar la entidad crítica para el acceso a las tareas, instalaciones, información o sistemas de control de las mismas.

3. Las solicitudes a que se refiere el apartado 1 serán canalizadas a través del CNPREC y se evaluarán en un plazo no superior a diez días desde la fecha de recepción de la solicitud.

4. La comprobación de antecedentes personales será proporcionada y se limitará estrictamente a determinar si por parte del Ministerio del Interior se considera la idoneidad o no de las personas evaluadas, con el único fin de evaluar un posible riesgo para la seguridad de la entidad crítica de que se trate, e incluirá las siguientes actuaciones:

a) Corroborar la identidad de la persona objeto de la comprobación de antecedentes.

b) Comprobar en el registro nacional o en el Sistema Europeo de Información de Antecedentes Penales los antecedentes penales y la eventual constancia de delitos directamente relacionados con las funciones del puesto concreto.

c) Comprobar la información de inteligencia relativa a indicios fundados de participación en actividades que constituyan amenazas directas para la seguridad de las infraestructuras críticas o activos críticos de la entidad. Su aplicación quedará limitada a las categorías de personal que el Plan de Resiliencia identifique expresamente para este nivel de comprobación.

cve: BOCG-15-A-88-1

Artículo 10. *Notificación de incidentes por las entidades críticas.*

1. Sin perjuicio de la obligación de comunicar el hecho tan pronto como sea conocida su ocurrencia, las entidades críticas notificarán 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 24 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. Estas notificaciones incluirán toda la información disponible necesaria para que la Secretaría de Estado de Seguridad pueda comprender la naturaleza, la causa y las posibles consecuencias del incidente, incluida cualquier información disponible que sea necesaria para determinar sus posibles repercusiones transfronterizas. Tales notificaciones no conllevarán una mayor responsabilidad para las entidades críticas.

2. A fin de determinar la magnitud de la perturbación, se tendrán en cuenta, en particular, los parámetros siguientes:

a) El número y el porcentaje de usuarios afectados.
b) Su duración.
c) La zona geográfica afectada, teniendo en cuenta si está aislada geográficamente.
d) El nivel de riesgo para la información y los datos personales.

3. Tan pronto como sea posible tras haber recibido la notificación a que se refiere el apartado 1, la Secretaría de Estado de Seguridad, a través del CNPREC, en su condición de punto de contacto único, facilitará a la entidad crítica afectada la información de seguimiento pertinente, incluida la que pueda respaldar una respuesta eficaz de la entidad crítica al incidente en cuestión. Por la misma vía, la Secretaría de Estado de Seguridad informará al público cuando considere que sea de interés general hacerlo.

4. Igualmente, sobre la base de la información facilitada por las notificaciones previstas en el apartado 1, la Secretaría de Estado de Seguridad, a través del CNPREC, informará al Sistema de Seguridad Nacional a través del Departamento de Seguridad Nacional, así como a los puntos de contacto únicos de los demás Estados miembros afectados en caso de que el incidente tenga o pueda tener repercusiones significativas en las entidades críticas y en la continuidad de la prestación de servicios esenciales para o en uno o varios Estados miembros.

El CNPREC tratará la información que envíe y reciba de conformidad con el derecho nacional y europeo, de forma que se respete su confidencialidad y se protejan la seguridad y los intereses comerciales de la entidad crítica de que se trate.

Asimismo, cuando un incidente tenga o pueda tener repercusiones significativas en la continuidad de la prestación de servicios esenciales en seis Estados miembros o más, la Secretaría de Estado de Seguridad lo notificará a la Comisión Europea.

5. La obligación de notificación de incidentes prevista en los apartados anteriores no obsta para el cumplimiento de cualquier otro deber legal de comunicación, en especial el deber de denuncia de aquellos hechos que revistan caracteres de delito ante las autoridades competentes, de acuerdo con lo dispuesto en la Ley de Enjuiciamiento Criminal.

Artículo 11. *Esquema nacional de certificación en materia de resiliencia de entidades críticas y normas de estandarización.*

1. Para el cumplimiento de lo establecido en esta ley, la Secretaría de Estado de Seguridad impulsará la implantación de un esquema nacional de certificación que permitirá evaluar y certificar el cumplimiento de los requisitos de resiliencia por parte de las entidades críticas.

cve: BOCG-15-A-88-1

2. El contenido del esquema nacional de certificación, así como el proceso de certificación, supervisión y pérdida de esta, serán los que se determinen reglamentariamente.

Este desarrollo reglamentario observará, al menos, los siguientes requisitos:

a) requisitos subjetivos: La certificación será expedida por entidades de certificación que hayan sido acreditadas por la Entidad Nacional de Acreditación (ENAC).

b) requisitos objetivos: La certificación acreditará la efectiva implantación de las medidas técnicas, organizativas, procedimentales u operativas de seguridad en cada una de las infraestructuras críticas operadas por la entidad correspondiente.

c) validez: La certificación tendrá una validez máxima de dos años, condicionada a la superación de las correspondientes auditorías de seguimiento.

3. Asimismo, se fomentará la utilización de normas y especificaciones técnicas nacionales, europeas e internacionales que sean pertinentes para las medidas de seguridad y resiliencia aplicables a las entidades críticas.

Sección 3.ª Procedimiento de identificación y catálogo nacional de entidades críticas y estratégicas

Artículo 12. *Identificación de las entidades críticas.*

1. La identificación y la designación de las entidades críticas de los sectores y subsectores estratégicos indicados en el anexo será realizada por la Comisión Nacional para la Protección y Resiliencia de las Entidades Críticas, a propuesta de la Secretaría de Estado de Seguridad, previa identificación provisional por el CNPREC.

2. Para la identificación de las entidades críticas se tendrán en cuenta los resultados de la Estrategia y la Evaluación Nacional de Amenazas y Riesgos, y se aplicarán, en concreto, todos los criterios siguientes:

a) Que la entidad preste uno o más servicios esenciales.

b) Que la entidad opere en el territorio nacional y sus infraestructuras críticas estén situadas en él.

c) Que un incidente tuviera efectos perturbadores significativos en la prestación por la entidad de uno o más servicios esenciales, en los términos del artículo 13, o en la prestación de otros servicios esenciales en los sectores indicados en el anexo, que dependan de dicho o dichos servicios esenciales

3. En el plazo de un mes desde su identificación como entidad crítica, a través del CNPREC, se notificará dicha circunstancia a la entidad afectada, así como las obligaciones que, en su caso, le incumben con arreglo a lo dispuesto en esta ley, y la fecha a partir de la cual le serán exigibles.

Artículo 13. *Efecto perturbador significativo.*

1. Para determinar el carácter significativo de un efecto perturbador, se tendrán en cuenta los siguientes criterios:

a) El número de usuarios que dependen del servicio esencial prestado por la entidad crítica de que se trate.

b) El grado en que otros sectores y subsectores indicados en el anexo dependen del servicio esencial que proporcionan.

c) Las repercusiones que los incidentes podrían tener, en términos de grado y duración, en las actividades económicas y sociales, el medio ambiente, la seguridad y la protección públicas o la salud de la población.

d) La cuota de mercado de la entidad en el mercado del servicio o servicios esenciales de que se trate.

cve: BOCG-15-A-88-1

e) La zona geográfica que podría verse afectada por un incidente, incluido cualquier repercusión transfronteriza, teniendo en cuenta la vulnerabilidad asociada al grado de aislamiento de ciertos tipos de zonas geográficas, como las regiones insulares, las regiones remotas o las zonas montañosas.

f) La importancia de la entidad para mantener un nivel suficiente de servicio esencial, teniendo en cuenta la disponibilidad de medios alternativos para la prestación de dicho servicio esencial.

2. Una vez identificadas las entidades críticas conforme a lo establecido en el artículo anterior, y a la mayor brevedad posible, la Secretaría de Estado de Seguridad trasladará al Consejo de Seguridad Nacional y a la Comisión Europea:

a) Una lista de servicios esenciales, en caso de haberse identificado servicios esenciales adicionales a los establecidos en los diferentes sectores y subsectores.

b) El número de entidades críticas identificadas para cada sector y subsector indicado en el anexo y para cada servicio esencial.

c) Los umbrales aplicados para especificar uno o varios de los criterios del apartado 1. Estos umbrales podrán presentarse como tales o de forma agregada.

Esta comunicación se renovará siempre que sea necesario y, en todo caso, como mínimo cada cuatro años.

Artículo 14. *Catálogo nacional de entidades críticas y estratégicas.*

1. La Secretaría de Estado de Seguridad elaborará, custodiará y mantendrá un catálogo de las entidades consideradas estratégicas. Asimismo, este catálogo incluirá, de forma expresa, las entidades que hayan sido identificadas como críticas conforme a lo establecido en el artículo 12.

2. El Catálogo integrará la información específica de todas las infraestructuras críticas y estratégicas que estén situadas en territorio nacional correspondientes a cada una de las entidades identificadas como críticas o estratégicas que operen en España. La información relativa a las infraestructuras críticas que forme parte del catálogo tendrá la calificación de secreto, conforme a lo dispuesto en la legislación en materia de secretos oficiales.

3. El Catálogo será revisado y actualizado siempre que resulte necesario y, en todo caso, con una periodicidad no superior a cuatro años. La identificación de nuevas entidades críticas se realizará conforme a los criterios establecidos en el artículo 12, y a partir de su designación y notificación a las entidades responsables, le resultará de aplicación las obligaciones contenidas en el artículo 7. Igualmente, a las entidades que después de una actualización dejen de estar identificadas como críticas o estratégicas, se les notificará dicha circunstancia, así como que dejan de estar sujetas a las obligaciones de esta ley a partir de la fecha de recepción de la comunicación.

CAPÍTULO III

Marco institucional para la protección y resiliencia de las entidades críticas

Artículo 15. *Autoridad nacional competente.*

1. Se designa a la Secretaría de Estado de Seguridad, en su calidad de órgano superior del Ministerio del Interior responsable en materia de protección y resiliencia de las entidades críticas, como autoridad nacional competente para la supervisión y cumplimiento de las disposiciones de esta ley, así como para la elaboración de la Estrategia Nacional de Protección y Resiliencia de las Entidades Críticas y de los planes estratégicos sectoriales; la elaboración y aprobación del Plan Nacional de Protección y Resiliencia de Entidades Críticas y de la Evaluación Nacional de Amenazas y Riesgos; y

cve: BOCG-15-A-88-1

la validación de la evaluación de riesgos por parte de las entidades críticas y de sus planes de resiliencia, y de los Planes de Apoyo Operativo.

2. Del mismo modo realizará la función de comunicación con la Comisión Europea y garantizará la consulta y cooperación con las autoridades nacionales pertinentes de otros Estados miembros, así como con las entidades críticas, las partes interesadas pertinentes, y con terceros países. También ejercerá la representación de España en el Grupo de Resiliencia de las Entidades Críticas, compuesto por representantes de los Estados miembros y de la Comisión Europea para facilitar la cooperación y el intercambio de información.

3. Respecto a las entidades críticas correspondientes a los sectores de banca, de los mercados financieros y de seguros, indicados en los puntos 3, 4 y 15 del anexo, las autoridades competentes serán las que correspondan con arreglo al artículo 46 del Reglamento (UE) 2022/2554. En el caso de las entidades críticas pertenecientes al sector de las infraestructuras digitales, indicado en el punto 7 del anexo, las autoridades competentes serán las autoridades de control designadas en la ley por la que se transponga la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022.

Artículo 16. *Punto de contacto único.*

1. Para el desempeño de sus funciones, la Secretaría de Estado de Seguridad contará con el apoyo del CNPREC, dependiente orgánicamente de la Dirección General de Coordinación y Estudios.

2. El CNPREC será el punto de contacto único de las entidades críticas con la Secretaría de Estado de Seguridad en lo relativo a sus responsabilidades, funciones y obligaciones en aquellas materias relacionadas con su protección y resiliencia. En el caso de las entidades críticas del sector público que estén vinculadas o dependan de una Administración Pública, el órgano competente de esta podrá erigirse, a través de aquel, en el interlocutor con la autoridad nacional.

3. Asimismo, el CNPREC se constituye como el punto de contacto único a los efectos de esta ley, siendo el órgano encargado de ejercer una función de enlace con el fin de garantizar la cooperación trasfronteriza con los puntos de contacto únicos de otros Estados miembros de la Unión Europea y con el Grupo de Resiliencia de las Entidades Críticas a que se refiere el artículo 19 de la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022.

Artículo 17. *Puntos de contacto especializados.*

1. Por cada uno de los sectores relacionados en el anexo se designará, al menos, un organismo, entidad u órgano de las Administraciones Públicas o de sus organismos públicos vinculados o dependientes, que será el encargado de impulsar, en el marco de sus competencias, las políticas de seguridad y resiliencia sobre los distintos sectores, subsectores y entidades críticas, y de velar por su aplicación, actuando en su ámbito como puntos de contacto especializados en la materia.

2. Respecto a las entidades críticas correspondientes a los sectores de banca, de los mercados financieros y de seguros, indicados en los puntos 3, 4 y 15 del anexo, esta función será desarrollada por quien corresponda con arreglo a su normativa específica. En el caso de las entidades críticas pertenecientes al sector de las infraestructuras digitales, indicado en el punto 7 del anexo, la función será asumida por los puntos de contacto sectoriales señalados en la ley por la que se transponga la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022.

cve: BOCG-15-A-88-1

Artículo 18. *Comisión Nacional para la Protección y Resiliencia de las Entidades Críticas.*

Como órgano colegiado adscrito a la Secretaría de Estado de Seguridad, la Comisión Nacional para la Protección y Resiliencia de las Entidades Críticas es el órgano competente para la aprobación de los planes estratégicos sectoriales elaborados por la Secretaría de Estado de Seguridad y colaborará con esta en la identificación de las entidades críticas, a través de su propuesta, de conformidad con lo previsto en el artículo 12. También será el órgano competente para la aprobación y modificación de la lista de los servicios esenciales. Sus funciones y composición serán las que reglamentariamente se establezcan.

Artículo 19. *Comité Interdepartamental para la Protección y Resiliencia de las Entidades Críticas.*

Para el cumplimiento de sus atribuciones, la Comisión Nacional para la Protección y Resiliencia de las Entidades Críticas contará con el apoyo del Comité Interdepartamental para la Protección y Resiliencia de las Entidades Críticas, cuyas funciones y composición se desarrollarán reglamentariamente. El Comité asistirá a la Secretaría de Estado de Seguridad en la elaboración de la Evaluación Nacional de Amenazas y Riesgos, la Estrategia Nacional de Protección y Resiliencia de las Entidades Críticas y de los planes estratégicos sectoriales y apoyará a la Secretaría de Estado de Seguridad en la elaboración de la Estrategia Nacional de Protección y Resiliencia de las Entidades Críticas.

Artículo 20. *Facultades de los Delegados y Delegadas del Gobierno.*

Los Delegados y las Delegadas del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía tendrán, bajo la autoridad de la persona titular de la Secretaría de Estado de Seguridad, en el ejercicio de sus atribuciones, las facultades que reglamentariamente se dispongan respecto de las infraestructuras críticas localizadas en su demarcación, operadas por entidades críticas. Entre estas facultades se incluirá, en todo caso, la de intervenir en su seguridad a través de la implantación y ejecución de los planes de apoyo operativo que elaboren las Fuerzas y Cuerpos de Seguridad.

Artículo 21. *Participación de las Comunidades Autónomas.*

1. Las Comunidades Autónomas con competencias estatutariamente asumidas para la protección de bienes y personas y el mantenimiento del orden público podrán desarrollar, sobre las infraestructuras críticas localizadas en su territorio, operadas por entidades críticas, las facultades que reglamentariamente se determinen respecto a su protección, sin perjuicio de los mecanismos de coordinación que se establezcan.

2. Las restantes Comunidades Autónomas participarán en la protección de las infraestructuras críticas, operadas por entidades críticas y localizadas en sus respectivos territorios, y en los órganos previstos en esta ley para la mejora de la resiliencia de las entidades críticas, de acuerdo con las competencias que les reconozcan sus respectivos estatutos de autonomía.

Artículo 22. *Actuaciones de colaboración y cooperación con las entidades críticas.*

1. Con el fin de aumentar la resiliencia de las entidades críticas, la Secretaría de Estado de Seguridad, con el apoyo de la Comisión Nacional para Protección y Resiliencia de las Entidades Críticas, colaborará permanentemente con las entidades críticas. Esta colaboración podrá incluir el desarrollo de materiales y metodologías de orientación, el apoyo a la organización de ejercicios para probar su resiliencia y evaluar

cve: BOCG-15-A-88-1

su capacidad de recuperación, la prestación de asesoramiento, formación y capacitación del personal de las entidades críticas, y cualquier otro que pueda redundar en la mejora de su resiliencia. Sin perjuicio de las normas aplicables en materia de ayudas estatales, se podrán proporcionar recursos financieros a las entidades críticas cuando sea necesario y esté justificado por objetivos de interés público.

2. La Secretaría de Estado de Seguridad garantizará la cooperación e intercambio de información y buenas prácticas con las entidades críticas de los sectores indicados en el anexo, y fomentará el intercambio voluntario de información, entre otras medidas, mediante mecanismos específicos para las entidades contempladas en la disposición adicional cuarta.

Artículo 23. *Cooperación entre Estados miembros de la Unión Europea.*

1. A través de la Secretaría de Estado de Seguridad se podrán realizar consultas reciprocas con otros Estados miembros de la Unión Europea en relación con las entidades críticas, con el fin de garantizar la aplicación coherente y coordinada de las disposiciones de esta ley y de las distintas normas nacionales por las que en cada uno de ellos se transponga la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022.

2. Dichas consultas tendrán lugar, en particular, en relación con las entidades críticas que:

a) Utilicen infraestructuras críticas que estén físicamente conectadas entre dos o más Estados miembros.

b) Formen parte de estructuras corporativas que estén conectadas o vinculadas a entidades críticas de otros Estados miembros.

c) Hayan sido identificadas como entidades críticas en un Estado miembro y presten servicios esenciales a otros Estados miembros o en otros Estados miembros.

3. Las consultas a que se refiere el apartado 1 tendrán como objetivo, entre otros, aumentar la resiliencia de las entidades críticas y, en la medida de lo posible, reducir la carga administrativa que soportan.

CAPÍTULO IV

Entidades críticas de especial importancia europea

Artículo 24. *Entidades críticas de especial importancia europea.*

1. Se considerará que una entidad crítica es de especial importancia europea cuando concurran los tres requisitos siguientes:

a) Haya sido identificada como entidad crítica.

b) Preste los mismos o similares servicios esenciales a o en seis o más Estados miembros.

c) Haya sido notificada su condición de entidad crítica de especial importancia europea, de conformidad con lo recogido en el apartado 4.

2. En el caso de que preste servicios esenciales a o en al menos seis Estados miembros, la entidad crítica identificada deberá informar a la Secretaría de Estado de Seguridad de los servicios esenciales que presta, así como de los Estados miembros donde los presta.

3. La Secretaría de Estado de Seguridad comunicará inmediatamente a la Comisión Europea y a los Estados miembros correspondientes aquellas entidades críticas que cumplen con los criterios establecidos para ser designadas como entidad crítica de especial importancia europea.

cve: BOCG-15-A-88-1

Asimismo, procederá a la coordinación con aquellos otros Estados miembros donde preste el servicio esencial.

4. Si la Comisión Europea determina que la entidad crítica en cuestión presta servicios esenciales a o en al menos seis Estados miembros, notificará a dicha entidad crítica, a través de la Secretaría de Estado de Seguridad, que se la ha identificado como una entidad crítica de especial importancia europea y, asimismo, las obligaciones que le incumben y la fecha a partir de la cual le serán exigibles.

5. Una vez que la Comisión Europea informe a la Secretaría de Estado de Seguridad que una entidad crítica ha sido identificada como entidad crítica de especial importancia europea, la Secretaría de Estado de Seguridad lo comunicará de forma inmediata a la entidad crítica.

Artículo 25. *Misiones de asesoramiento.*

1. Cuando una entidad crítica haya sido identificada como de especial importancia europea, la Secretaría de Estado de Seguridad podrá solicitar a la Comisión Europea que organice una misión de asesoramiento para evaluar las medidas adoptadas por la entidad crítica, con el fin de cumplir con las obligaciones recogidas en esta ley.

2. La Comisión Europea podrá organizar una misión de asesoramiento, a iniciativa propia o a petición de uno o más Estados miembros a o en los que se preste el servicio esencial, siempre que cuente con el acuerdo del Estado miembro que haya identificado una entidad crítica de especial importancia europea como entidad crítica.

3. Cuando una entidad crítica de especial importancia europea haya sido identificada en España, la Secretaría de Estado de Seguridad, previa solicitud motivada de la Comisión Europea o de uno o varios de los Estados miembros a o en los que se preste el servicio esencial, facilitará a la Comisión Europea la siguiente información:

a) La evaluación de riesgos de la entidad crítica.
b) Las medidas adoptadas.
c) Las medidas de supervisión o ejecución contempladas en el artículo 26.

Igualmente, en caso de tratarse de una entidad que haya sido identificada en otro Estado miembro, pero preste un servicio esencial a o en España, la Secretaría de Estado de Seguridad podrá, motivadamente, solicitar, en idénticos términos, que el Estado miembro que la haya identificado facilite a la Comisión Europea la misma información.

4. La misión de asesoramiento informará de sus conclusiones a la Comisión Europea, al Estado miembro que haya identificado a la entidad crítica de especial importancia europea, a los Estados miembros en los que se preste el servicio esencial y a la entidad crítica en cuestión, en el plazo de tres meses a partir de la conclusión de la misión de asesoramiento.

En el caso de tratarse de una entidad identificada en España o cuando el servicio esencial se preste a o en España, la Secretaría de Estado de Seguridad analizará el citado informe y, en caso necesario, informará a la Comisión Europea sobre el cumplimiento o no por parte de esta de sus obligaciones y, si ha lugar, sobre las medidas que podrían adoptarse para aumentar su resiliencia.

En los supuestos a los que se refiere el párrafo anterior, la Comisión Europea comunicará a la Secretaría de Estado de Seguridad y a dicha entidad crítica su dictamen sobre el cumplimiento o no de sus obligaciones y, en su caso, sobre las medidas que podrían adoptarse para aumentar su resiliencia.

La Secretaría de Estado de Seguridad tendrá en cuenta el dictamen mencionado y se asegurará de que también sea tenido en consideración por la entidad crítica, e informará, a la Comisión Europea y a los Estados miembros en o a los que se preste el servicio esencial de las medidas adoptadas de conformidad con dicho dictamen.

5. Cuando se trate de una entidad identificada en España o cuando el servicio esencial se preste a o en España, la Secretaría de Estado de Seguridad podrá proponer a la Comisión Europea candidatos a formar parte de la misión de asesoramiento para su

cve: BOCG-15-A-88-1

selección. Cuando sea necesario, los miembros de la misión de asesoramiento deberán disponer de la habilitación de seguridad suficiente, teniendo en cuenta la normativa sobre protección de la información que resulte aplicable en cada caso.

6. Las entidades críticas de especial importancia europea proporcionarán a la misión de asesoramiento acceso a la información, los sistemas y las instalaciones relacionados con la prestación de sus servicios esenciales que resulte necesario para llevar a cabo su función.

7. Las misiones de asesoramiento que se realicen en España se practicarán de conformidad con el ordenamiento jurídico español, con respecto a la responsabilidad del Estado en materia de seguridad nacional y a la protección de los intereses de seguridad.

8. Cuando la misión de asesoramiento se haya desarrollado en territorio nacional, la Secretaría de Estado de Seguridad informará al Grupo de Resiliencia de las Entidades Críticas de la Unión Europea sobre las conclusiones principales y sobre la experiencia adquirida, con vistas a fomentar el aprendizaje mutuo.

CAPÍTULO V

Supervisión y régimen sancionador

Sección 1.ª Potestades de supervisión

Artículo 26. *Actividades de supervisión de las entidades críticas.*

1. Las actividades de supervisión de las entidades críticas, a fin de evaluar el cumplimiento de las obligaciones establecidas en esta ley, se realizarán por la Secretaría de Estado de Seguridad.

2. Para el desarrollo de estas actividades, la Secretaría de Estado de Seguridad tendrá las siguientes facultades:

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. A tales efectos, podrá acordar la realización de planes de auditoría preventiva, referidos a las actividades de una entidad crítica o de un sector concreto de actividad, para el análisis del cumplimiento de las disposiciones de esta ley.

d) Impartir directrices generales o específicas para el mejor cumplimiento de las obligaciones de esta ley.

Para el desempeño de sus funciones de supervisión, las entidades críticas deberán prestar a la Secretaría de Estado de Seguridad la colaboración necesaria y facilitarle el acceso a la información, sistemas e instalaciones relacionados con la prestación de los servicios esenciales.

3. En relación con las entidades esenciales e importantes conforme a la ley por la que se transponga 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:

a) La información necesaria para evaluar si las medidas adoptadas para garantizar su resiliencia cumplen con los requisitos establecidos en el artículo 8.

b) Las pruebas de la aplicación efectiva de dichas medidas, incluidos los resultados de una auditoría realizada por un auditor cualificado e independiente seleccionado por la entidad y a expensas de ésta.

cve: BOCG-15-A-88-1

Cuando se exija dicha información, la Secretaría de Estado de Seguridad con arreglo a esta ley indicará con qué objeto la pide y especificará la información requerida.

4. Tras las actividades de supervisión a que se refiere el apartado 2 o, en su caso, la evaluación de la información obtenida en virtud del apartado 3, y sin perjuicio del ejercicio de las potestades sancionadoras, la Secretaría de Estado de Seguridad podrá requerir a la entidad crítica correspondiente para que adopte las medidas necesarias y proporcionadas para subsanar los incumplimientos detectados, en el plazo razonable que se le conceda al efecto. Dicho requerimiento tendrá en cuenta, en particular, la gravedad del incumplimiento.

No obstante, cuando se trate de la evaluación del cumplimiento de sus obligaciones por parte de aquellas entidades críticas que también sean entidades esenciales e importantes de acuerdo con la ley por la que se transponga la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, la Secretaría de Estado de Seguridad informará a la autoridad competente designada de conformidad con la mencionada ley, y estará facultada para requerir de esta que ejerza sus potestades de supervisión y ejecución en relación con la referida entidad crítica. A tal efecto, la Secretaría de Estado de Seguridad cooperará e intercambiará información con la autoridad nacional competente conforme a la ley por la que se transponga la mencionada directiva.

Las autoridades competentes estarán facultadas para fijar un plazo en el que la entidad crítica deberá adoptar las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de dichas autoridades. Si las medidas requeridas no se adoptan dentro del plazo establecido, las autoridades competentes estarán facultadas para:

a) Suspender temporalmente o solicitar al organismo de certificación, de conformidad con el ordenamiento jurídico, que suspenda temporalmente una certificación o autorización referente a una parte o la totalidad de los servicios o actividades de que se trate prestados por la entidad crítica.

b) Solicitar a los órganos jurisdiccionales competentes que prohíban temporalmente a cualquier persona que ejerza responsabilidades de dirección a nivel de director general o representante legal de dicha entidad crítica, ejercer funciones de dirección o representación en dicha entidad.

5. El intercambio de la información que se considere confidencial o haya sido clasificada de acuerdo con las normas vigentes en cada caso se realizará únicamente cuando sea necesario para la aplicación de esta ley, y se limitará a aquella que sea pertinente y proporcionada para la finalidad de dicho intercambio. El ejercicio de las facultades de supervisión a que se refiere este artículo se ejercerá con las salvaguardias adecuadas. En particular, garantizando la preservación de la confidencialidad de la información, su seguridad y los intereses comerciales de las entidades críticas, respetando al mismo tiempo la seguridad del Estado y los derechos fundamentales de las personas que pudieran resultar afectadas, incluido el derecho de las entidades críticas a ser oídas.

Sección 2.ª Reglas generales

Artículo 27. *Sujetos responsables.*

1. La responsabilidad por las infracciones previstas recaerá en las entidades críticas autoras del hecho en que consista la infracción. Solo podrá exigirse responsabilidad a las entidades críticas por estas infracciones cuando en su conducta concurra dolo o culpa.

2. Sin perjuicio de la responsabilidad que corresponda a las entidades obligadas, quienes ejerzan en la misma cargos de administración o dirección, sean unipersonales o colegiados, serán responsables subsidiariamente de las infracciones cuando éstas sean imputables a su conducta dolosa o negligente.

cve: BOCG-15-A-88-1

Artículo 28. *Competencia sancionadora.*

La imposición de sanciones por las infracciones previstas en esta ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Interior, y en el caso de infracciones graves y leves, a la persona titular de la Secretaría de Estado de Seguridad.

Artículo 29. *Criterios de graduación de las sanciones.*

Para la graduación de la sanción aplicable en cada caso se tomarán en consideración los siguientes criterios:

a) La naturaleza, gravedad y duración de la infracción.
b) El grado de culpabilidad o la existencia de intencionalidad.
c) La reincidencia, cuando en el término de dos años se hubiera cometido al menos otra infracción de la misma naturaleza, y así se haya declarado por resolución firme en vía administrativa.
d) La naturaleza, el tamaño y la solidez financiera de la entidad.
e) El nivel de cooperación con las autoridades competentes.
f) El grado de obstrucción a las auditorías o actividades de control ordenadas por la autoridad competente tras la constatación de un incumplimiento.
g) El perjuicio material o inmaterial causado, incluidas las pérdidas financieras o económicas, los efectos para otros servicios, el número de usuarios afectados y el grado de afectación a la prestación del servicio esencial.
h) Las medidas adoptadas por la entidad para prevenir o reducir los perjuicios materiales o inmateriales.
i) El grado de responsabilidad de la entidad, teniendo en cuenta las medidas técnicas y organizativas adoptadas para cumplir con lo dispuesto en esta ley.

Sección 3.ª Infracciones y sanciones

Artículo 30. *Clasificación de las infracciones.*

Las infracciones tipificadas en esta ley se clasifican en muy graves, graves y leves.

Artículo 31. *Infracciones muy graves.*

Son infracciones muy graves:

a) El incumplimiento de la obligación de notificar incidentes previstos en el artículo 10.1 dentro del plazo de 24 horas desde su conocimiento o desde que hubieran debido conocerse, si causan un riesgo o perjuicio muy grave a la prestación de los servicios esenciales, teniendo en cuenta los parámetros de magnitud previstos en el artículo 10.2.
b) La carencia de las medidas de resiliencia comprendidas en los artículos 6, 8 y 11 o no tenerlas efectivamente implantadas, cuando cause un riesgo o perjuicio muy grave a los servicios esenciales, teniendo en cuenta el grado de la perturbación provocada en atención a los criterios contemplados en el artículo 13.1.
c) El incumplimiento por parte de las entidades críticas de los deberes de colaboración con las funciones de supervisión de la autoridad competente o con las misiones de inspección, cuando impida el ejercicio de las funciones de supervisión o inspección.
d) La aportación de datos falsos a las entidades de certificación para obtener certificaciones del cumplimiento de los requisitos de resiliencia y la emisión de certificaciones a sabiendas de que se han proporcionado datos falsos para su obtención.
e) La falta de cumplimiento, en el plazo concedido al efecto, de las medidas para la mejora de la resiliencia o la subsanación de los incumplimientos detectados, exigidas

cve: BOCG-15-A-88-1

tras la realización de actividades de supervisión o, cuando se trate de entidades críticas de especial importancia europea, las propuestas por la Comisión Europea, en su caso.

Artículo 32. *Infracciones graves.*

Son infracciones graves:

a) El incumplimiento de la obligación de notificar incidentes previstos en el artículo 10.1 dentro del plazo de 24 horas desde su conocimiento o desde que hubieran debido conocerse, si causan un riesgo o perjuicio grave a la prestación de los servicios esenciales, teniendo en cuenta los parámetros de magnitud previstos en el artículo 10.2.

b) La carencia de las medidas de seguridad previstas en los artículos 6, 8 y 11 o no tenerlas efectivamente implantadas cuando cause un riesgo o perjuicio grave a la prestación de los servicios esenciales, teniendo en cuenta el grado de la perturbación provocada en atención a los criterios contemplados en el artículo 13.2.

c) El incumplimiento por parte de las entidades críticas de los deberes de colaboración con las funciones de supervisión de la autoridad competente o con las misiones de inspección, cuando sin haber impedido el ejercicio de las funciones de supervisión o inspección, lo haya entorpecido.

d) La falta de elevación a la Secretaría de Estado de Seguridad, en el plazo máximo de nueve meses posteriores a la notificación de su identificación como entidad crítica, de la evaluación de riesgos en los términos previstos en el artículo 6.1.

e) La falta de elaboración o de renovación del plan de resiliencia de la entidad crítica en el plazo señalado en el artículo 8.

f) La falta de obtención o de renovación de la certificación prevista en el artículo 11, en el plazo que se determine reglamentariamente.

g) La falta de diligencia en la verificación de la información por parte de la empresa certificadora, antes de la emisión del certificado.

h) La falta de información a la Secretaría de Estado de Seguridad, en caso de que preste servicios esenciales en al menos seis Estados miembros, de los servicios esenciales que presta en tales Estados, y de los Estados a los que presta tales servicios esenciales en los términos previstos en el artículo 24.2.

i) La falta de designación de una persona como responsable de seguridad y resiliencia o la carencia de la habilitación exigida, así como la falta de designación del delegado de seguridad de una infraestructura crítica o la no constitución del Área de Seguridad, a los que se refiere el artículo 8.3.

j) El cumplimiento deficiente, en el plazo concedido al efecto, de las medidas para la mejora de la resiliencia o la subsanación de los incumplimientos detectados, exigidas tras la realización de actividades de supervisión o, cuando se trate de entidades críticas de especial importancia europea, las propuestas por la Comisión, en su caso.

Artículo 33. *Infracciones leves.*

Son infracciones leves:

a) El incumplimiento de la obligación de notificar incidentes previstos en el artículo 10.1 perturbadores en la prestación de los servicios esenciales dentro del plazo de 24 horas desde su conocimiento o desde que hubieran debido conocerse, siempre que no causen un riesgo o perjuicio muy grave o grave a la prestación de los servicios esenciales, teniendo en cuenta los parámetros de magnitud previstos en el artículo 10.2 o de la obligación de comunicar el hecho tan pronto como sea conocida su ocurrencia.

b) La falta de comunicación de la designación o renovación de la persona, unidad u órgano responsable de seguridad y resiliencia de la entidad crítica o del delegado de seguridad de cada infraestructura crítica.

cve: BOCG-15-A-88-1

c) La no remisión del informe detallado de un incidente a la Secretaría de Estado de Seguridad dentro del plazo recogido en el artículo 10 o que no incluya la información mencionada en el mismo.

d) El cumplimiento deficiente de los deberes de colaboración con las funciones de supervisión de la autoridad competente o con las misiones de inspección, siempre que la conducta no sea constitutiva de infracción muy grave o grave.

Artículo 34. *Sanciones.*

1. Las infracciones muy graves se sancionarán con multa de 1.000.001 euros hasta 10.000.000 euros o una cuantía equivalente de hasta el 2 por ciento del volumen de negocios anual total a nivel mundial de la empresa a la que pertenece la entidad crítica durante el ejercicio financiero anterior, optándose por la de mayor cuantía.

2. Las infracciones graves se sancionarán con multa de 100.001 euros hasta 1.000.000 euros.

3. Las infracciones leves se sancionarán con multa de 10.000 euros hasta 100.000 euros.

4. Siempre que se garantice la prestación de los correspondientes servicios esenciales, la multa podrá llevar aparejada alguna o algunas de las siguientes sanciones accesorias, atendiendo a la naturaleza de los hechos constitutivos de la infracción,

a) La suspensión temporal de las licencias, autorizaciones o permisos desde seis meses y un día a dos años por infracciones muy graves y hasta seis meses para las infracciones graves. En caso de reincidencia, la sanción podrá ser de dos años y un día hasta seis años por infracciones muy graves y hasta dos años por infracciones graves.

b) La clausura de las fábricas, locales o establecimientos, desde seis meses y un día a dos años por infracciones muy graves y hasta seis meses por infracciones graves. En caso de reincidencia, la sanción podrá ser de dos años y un día hasta seis años por infracciones muy graves y hasta dos años por infracciones graves.

5. Las sanciones firmes en vía administrativa por infracciones muy graves y graves podrán ser publicadas, a costa del sancionado, en el «Boletín Oficial del Estado» y en el portal de internet de la autoridad competente, en atención a los hechos concurrentes.

Artículo 35. *Prescripción de las infracciones.*

1. Las infracciones prescribirán a los seis meses, a los dos años o a los tres años de haberse cometido, según sean leves, graves o muy graves, respectivamente.

2. Los plazos se computarán desde el día en que se haya cometido la infracción. No obstante, en los casos de infracciones continuadas y de infracciones de efectos permanentes, los plazos se computarán, respectivamente, desde que finalizó la conducta infractora o el último acto con el que la infracción se consumó.

3. Se interrumpirá, igualmente, la prescripción como consecuencia de la apertura de diligencias de investigación por el Ministerio Fiscal o de un procedimiento judicial penal por los mismos hechos, hasta que la autoridad judicial comunique al órgano administrativo su finalización. En tal supuesto el órgano administrativo se abstendrá de seguir el procedimiento sancionador mientras la autoridad judicial no dicte sentencia firme o resolución que ponga fin al procedimiento penal, o el Ministerio Fiscal no acuerde la improcedencia de iniciar o proseguir las actuaciones en vía penal, quedando hasta entonces interrumpido el plazo de prescripción.

La autoridad judicial o, en su caso, el Ministerio Fiscal comunicarán al órgano administrativo la resolución o acuerdo que se hubiera adoptado.

Artículo 36. *Prescripción de las sanciones.*

1. Las sanciones impuestas por infracciones muy graves prescribirán a los tres años, las impuestas por infracciones graves, a los dos años, y las impuestas por

cve: BOCG-15-A-88-1

infracciones leves, al año, computados desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

2. La prescripción de las infracciones y sanciones se regirá por lo dispuesto en el artículo 30 de la Ley 40/2015 de 1 de octubre de Régimen Jurídico del Sector Público.

Sección 4.ª Procedimiento sancionador

Artículo 37. *Régimen jurídico.*

El ejercicio de la potestad sancionadora se regirá por lo establecido en la Ley 39/2015, de 1 octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 octubre, sin perjuicio de las especialidades que se regulan en este capítulo.

Artículo 38. *Concurrencia de infracciones.*

1. No podrán sancionarse hechos que ya hayan sido sancionados penal o administrativamente cuando se aprecie identidad de sujeto, hecho y fundamento jurídico.

2. Cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de estos a los órganos u organismos a los efectos de iniciar, en su caso, el oportuno procedimiento sancionador.

Artículo 39. *Subordinación del procedimiento administrativo sancionador respecto del penal.*

1. Los hechos declarados probados por resoluciones judiciales penales firmes vincularán al órgano administrativo respecto de todos los procedimientos sancionadores que se sustancien.

2. En caso de no haberse estimado la existencia de ilícito penal, o haberse dictado resolución de otro tipo que ponga fin al procedimiento penal, podrá iniciarse o proseguir el procedimiento sancionador.

3. En cualquiera de los casos anteriores, la autoridad judicial o el Ministerio Fiscal comunicarán al órgano administrativo la resolución o acuerdo que hubieran adoptado, a fin de proseguir o no con el correspondiente procedimiento sancionador.

Artículo 40. *Medidas provisionales.*

1. Se podrán adoptar medidas provisionales, de conformidad con el artículo 56.1 de la Ley 39/2015, de 1 octubre, que deberán ser ratificadas, modificadas o revocadas en el acuerdo de incoación del procedimiento, en el plazo máximo de quince días desde la adopción de estas. Asimismo, antes de la iniciación del procedimiento, el órgano competente para iniciar o instruir el procedimiento podrá adoptar las medidas provisionalísimas en los términos del apartado segundo del citado precepto.

2. Las medidas provisionales previstas en este artículo no serán aplicables a las entidades del Sector Público sujetas a lo dispuesto en esta ley.

Artículo 41. *Caducidad del procedimiento.*

1. El procedimiento caducará transcurrido un año desde su incoación sin que se haya notificado la resolución. En los supuestos en los que el procedimiento se hubiera paralizado por causa imputable al interesado, o por la existencia de un procedimiento judicial penal por los mismos hechos, se interrumpirá el cómputo del plazo para resolver y notificar la resolución.

cve: BOCG-15-A-88-1

2. La resolución que declare la caducidad se notificará al interesado y pondrá fin al procedimiento, sin perjuicio de que la Administración pueda acordar la incoación de un nuevo procedimiento en tanto no haya prescrito la infracción.

3. Los procedimientos caducados no interrumpirán el plazo de prescripción.

Disposición adicional primera. *No incremento de gasto público.*

Las medidas contempladas en esta ley no generarán incremento de dotaciones ni de retribuciones, ni de otros gastos de personal al servicio del sector público.

Disposición adicional segunda. *Medios de transmisión.*

Las comunicaciones que se regulan en esta ley se efectuarán conforme a los procedimientos desarrollados reglamentariamente y, en lo que resulte aplicable, al Esquema Nacional de Seguridad y al Esquema Nacional de Interoperabilidad.

Disposición adicional tercera. *Protección de datos de carácter personal.*

1. Los tratamientos de datos personales por parte de las autoridades competentes en materia de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública, se regirán por lo dispuesto en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales cuando se lleven a cabo legitimadas conforme al artículo 11 de la citada ley orgánica.

Las operaciones de tratamiento llevadas a cabo por las autoridades competentes para el tratamiento INCOA y aquellas llevadas a cabo en virtud del artículo 26 quedan dentro el ámbito de aplicación de esta Ley Orgánica, salvo las que se hallen sometidas a la normativa sobre secretos oficiales y materias clasificadas.

El ejercicio de los derechos de información, acceso, rectificación, supresión de datos personales, limitación de su tratamiento y no ser objeto de decisiones totalmente automatizadas, se regirá por lo dispuesto en los artículos 20 a 26 de la Ley Orgánica 7/2021, de 26 de mayo, salvo lo que queda sometido a la normativa de secretos oficiales y materias clasificadas.

2. Los tratamientos de datos personales por parte de las entidades críticas, en aplicación de esta ley, se regirán por lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Las operaciones de tratamiento derivadas de la implantación de sistemas de autenticación y reconocimiento biométricos se llevarán a cabo conforme al artículo 6.1 c), en correspondencia con los artículos 9 y 22.2 b) y 4, del Reglamento General de Protección de datos.

En estos casos, el ejercicio de los derechos de información, acceso, rectificación, supresión de datos personales, oposición, portabilidad, limitación de su tratamiento y no ser objeto de decisiones totalmente automatizadas, se regirá por lo dispuesto en los artículos 13 a 22 del Reglamento General de Protección de Datos.

Disposición adicional cuarta. *Entidades críticas del sector de banca, de seguros, de las infraestructuras de los mercados financieros y de las infraestructuras digitales.*

Las disposiciones contenidas en los artículos 6, 7.3, 8, 9, 10, 11, 23, 24 y 25 y en el capítulo V no serán de aplicación a las entidades críticas identificadas conforme a lo

cve: BOCG-15-A-88-1

dispuesto en el artículo 12, en los sectores de banca, de seguros, de las infraestructuras de los mercados financieros y de las infraestructuras digitales, definidos conforme a lo dispuesto en los puntos 3, 4, 7 y 15 del anexo.

No obstante, podrán adoptarse disposiciones destinadas a alcanzar un mayor nivel de resiliencia de dichas entidades, siempre que resulten coherentes con el Derecho comunitario que les sea aplicable.

Disposición adicional quinta. *Informes y comprobaciones para acreditaciones y antecedentes.*

1. La Dirección General de Coordinación y Estudios de la Secretaría de Estado de Seguridad, en virtud de sus competencias de coordinación y desarrollo de los planes directores y operativos de la Secretaría de Estado en materia de seguridad ciudadana, coordinando la actuación de las Fuerzas y Cuerpos de Seguridad del Estado en este ámbito, así como de éstos con las policías autonómicas y las policías locales, tendrá la condición de responsable del tratamiento denominado Informes y comprobaciones para acreditaciones y antecedentes.

2. La finalidad perseguida con el tratamiento es que las Fuerzas y Cuerpos de Seguridad competentes puedan realizar las comprobaciones necesarias para emitir informes que permitan expedir acreditaciones o informes de identidad y/o idoneidad para prevenir y detectar ilícitos penales en los supuestos de acceso a:

a) Zonas restringidas por la normativa de seguridad aérea y portuaria y por la de infraestructuras ferroviarias

b) Zonas restringidas por la normativa de seguridad nuclear.

c) Zonas restringidas por la normativa de Entidades Criticas y Ciberseguridad.

d) Zonas de seguridad en eventos cuya seguridad corresponda a las Fuerzas y Cuerpos de Seguridad.

e) Recintos o instalaciones de Fuerzas Armadas conforme a la normativa de seguridad y defensa nacional

3. En el tratamiento, informes y comprobaciones para acreditaciones y antecedentes, se podrán tratar los datos relativos a la identidad de las personas, datos de contacto, dirección, residencia, datos laborales, sus antecedentes penales e información de inteligencia, los datos personales de identidad y contacto de los responsables, gestores y usuarios del fichero del tratamiento.

4. Se podrán ceder datos a los órganos jurisdiccionales del orden penal, el Ministerio Fiscal y las Fuerzas y Cuerpos de Seguridad, así como otras entidades cuando se prevea legalmente.

En los casos en los que el tratamiento consista en remitir a las entidades únicamente el resultado de la evaluación de idoneidad para proceder acreditar o permitir el acceso a las personas interesadas, la información sobre el parecer negativo o positivo de la comprobación se transmitirá a:

a) La Agencia Estatal de Seguridad Área, gestores portuarios y aeroportuarios, compañías aéreas y proveedores de servicios de navegación aérea cuando se trate de procesos de comprobación de idoneidad para acceder a zonas restringidas aeroportuarias y portuarias. Y la Agencia Estatal de Seguridad Ferroviaria, Administradores de Infraestructuras Ferroviarias, empresas ferroviarias y proveedores de servicios ferroviarios cuando se trate de procesos de comprobación de idoneidad para acceder a zonas de acceso restringido en las infraestructuras ferroviarias.

b) Titulares de instalaciones nucleares cuando se proceda a evaluar la idoneidad del personal que acceda a las zonas restringidas de instalaciones nucleares.

c) Titulares de entidades críticas, esenciales o importantes en el marco de la ciberseguridad cuando se proceda a evaluar la idoneidad para el acceso a sus instalaciones críticas, esenciales o importantes.

cve: BOCG-15-A-88-1

d) Responsables de seguridad de las Fuerzas Armadas para evaluar la idoneidad en el acceso a sus instalaciones.

6. Los destinatarios serán también responsables del tratamiento de los datos que hubiera sido objeto de comunicación conforme a las disposiciones de esta ley y a la normativa que les resulte de aplicación por el mismo tratamiento.

7. La base jurídica de las autoridades competentes se ajusta a lo dispuesto en el artículo 11 de la Ley Orgánica 7/2021, de 26 de mayo, incluidas la protección y prevención frente a las amenazas contra la seguridad pública sin perjuicio de la aplicación a su tratamiento de la legislación reguladora del ejercicio de la potestad jurisdiccional o las que en su caso resultaren de aplicación.

En el caso de las personas a las que se les obliga o habilita a solicitar una evaluación de idoneidad, la base de legitimación es la contenida en el artículo 9.

8. Los datos recogidos se limitarán a los necesarios para el cumplimiento de las finalidades descritas, de acuerdo con el principio de minimización de datos.

9. La recolección de datos se hará conforme a la legislación vigente con especial atención al cumplimiento del deber de información previa a los interesados sobre las condiciones, derechos y obligaciones del tratamiento, así como a los posibles destinatarios en los términos previstos en la ley.

10. De acuerdo con la finalidad del tratamiento, se conservarán los datos recogidos durante el tiempo necesario para el cumplimiento del fin para el cual fueron recogidos en virtud del artículo 8 de la Ley Orgánica 7/2021, de 26 de mayo, y en su caso por el tiempo necesario para atender a las responsabilidades derivadas de su tratamiento ante los órganos administrativos o jurisdiccionales competentes. Una vez trascurrido dicho periodo de conservación, los datos serán suprimidos de manera que se imposibilite la correlación o identificación de estos con los interesados.

Los responsables de tratamiento de los sujetos obligados que tengan la obligación o la habilitación para solicitar una evaluación de idoneidad deberán determinar el plazo máximo de conservación necesarios de sus procesos en virtud de la necesidad de su conservación. En todo caso, el plazo no podrá exceder de 3 años.

11. El responsable de tratamiento cuando sea una autoridad competente de la Ley Orgánica 7/2021, de 26 de mayo, deberá garantizar la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta, en todo caso, lo previsto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

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

12. El ejercicio de derechos por las personas físicas sujetas a la normativa de protección de datos se garantizará conforme a dicha normativa. Serán atendidas las solicitudes para el ejercicio de tales derechos por el responsable del tratamiento en los términos establecidos en la legislación vigente de conformidad con cada uno de los supuestos concretos previstos y en el momento procesal correspondiente. El resto de los derechos se ejercerán conforme a la normativa específica aplicable.

Disposición adicional sexta. *Obligaciones de comunicación.*

La Secretaría de Estado de Seguridad deberá comunicar a la Comisión Europea:

a) En el plazo de tres meses, desde la entrada en vigor de esta ley, comunicará la identidad de la autoridad nacional competente y del punto de contacto único, sus funciones y responsabilidades, así como sus datos de contacto. Cualquier modificación posterior de estos datos también deberá ser notificada.

cve: BOCG-15-A-88-1

b) Con la mayor inmediatez posible y, como mínimo, cada cuatro años, trasladará una lista con los servicios esenciales adicionales determinados que completen la lista de servicios esenciales, el número de entidades críticas identificadas para cada sector y subsector estratégico indicado en el anexo y para cada servicio esencial y los umbrales aplicados para especificar uno o varios de los criterios de efectos perturbadores significativos. Estos umbrales podrán presentarse como tales o de forma agregada.

c) Antes del 17 de julio de 2028, y posteriormente cada dos años, presentará, a través del CNPREC, al Grupo de Resiliencia de las Entidades Críticas un informe de síntesis sobre las notificaciones de cooperación transfronteriza recibidas, incluido el número de notificaciones, la naturaleza de los incidentes notificados y las medidas adoptadas.

d) De forma inmediata a la publicación de esta ley, el régimen sancionador establecido en él y las medidas adoptadas en ese ámbito, así como cualquier modificación posterior de dicho régimen o medidas, que se comunicarán sin demora.

Disposición adicional séptima. *Instalación de sistemas de autenticación y reconocimiento biométricos.*

1. En virtud de lo dispuesto en el artículo 26 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, y teniendo en cuenta la Evaluación Nacional de Amenazas y Riesgos, las entidades críticas podrán establecer sistemas de reconocimiento biométrico de identificación o autenticación en todas o algunas de sus instalaciones con objeto de garantizar el control de accesos y el desplazamiento con fines de prevención de delitos y seguridad física.

La implantación de estos sistemas, las características que deben reunir y su extensión, se regularán mediante real decreto aprobado por el Consejo de Ministros.

2. El tratamiento datos a desarrollar por cada uno de los responsables es necesario para garantizar el funcionamiento de las entidades críticas ante cualquier ataque o amenaza y se legitima en el artículo 6.1 c), en relación con el artículo 9.2. b) y g) del Reglamento General de Protección de Datos.

3. El sistema de reconocimiento biométrico permitirá autenticar e identificar en cada caso a las personas que accedan a las instalaciones y aquellas que se desplacen por las mismas en los lugares o emplazamientos que lo hagan necesario con finalidad de garantizar la seguridad. El único objetivo del tratamiento será confirmar que una persona física es quien dice ser para acceder o desplazarse por las instalaciones o que está habilitada para ello mediante un acceso de seguridad los locales de instalaciones críticas. Estos tratamientos no se podrán emplear para fines laborales o de control de jornada.

4. El sistema atenderá a los principios de privacidad por diseño y minimización. La tecnología elegida debe adecuarse a las necesidades concretas en virtud del tipo y características de la entidad o instalación, de manera que se demuestre que no exige recogida o cualquier otro tratamiento innecesario de datos Es obligatorio la realización previa de una Evaluación de Impacto para la protección de datos.

5. Los tratamientos llevados a cabo permitirán la posibilidad de revocar el vínculo de identidad entre la plantilla biométrica y la persona física, implementarán medios técnicos que imposibiliten el empleo de las plantillas para otros usos, emplearán el cifrado adecuado y utilizarán datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.

6. Estos sistemas no podrán adoptar decisiones totalmente automatizadas y en el supuesto de que se empleen sistemas de inteligencia artificial, los procesos control de acceso y presencia en las instalaciones se adecuarán al contenido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013,

cve: BOCG-15-A-88-1

(UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

7. Las personas interesadas dispondrán de información previa y suficiente para ser conscientes del riesgo que supone el tratamiento de sus datos biométricos, especialmente si se encuentran en una situación de vulnerabilidad. La toma de los datos se realizará de forma consciente e informada, dejando constancia en derecho de esta actuación.

8. Los datos biométricos se suprimirán cuando no se vinculen a la finalidad que motivo el tratamiento.

Disposición adicional octava. *Instalación de sistemas antidrones.*

En virtud de lo dispuesto en el artículo 26 de la Ley Orgánica 4/2015, de 30 de marzo, y teniendo en cuenta la Evaluación Nacional de Amenazas y Riesgos, las entidades críticas podrán instalar sistemas antidrones en todas o algunas de sus instalaciones con objeto de garantizar su protección. La implantación de estos sistemas, las características que deben reunir y su extensión, se regularán mediante real decreto aprobado por el Consejo de Ministros.

Disposición adicional novena. *Coordinación con mecanismos estratégicos de capacidad industrial nacional y de reservas energéticas.*

En el marco de la evaluación de riesgos de las entidades críticas, y sin perjuicio de las competencias de los departamentos ministeriales correspondientes, se podrá prever la coordinación con mecanismos estratégicos de capacidad industrial nacional, tales como la Reserva Estratégica basada en las Capacidades Nacionales de Producción Industrial (RECAPI) y la Corporación de Reservas Energéticas de Productos Petrolíferos (CORES), a efectos de garantizar la disponibilidad de recursos esenciales ante escenarios de disrupción identificados.

Disposición transitoria única. *Aplicación transitoria del sistema de planificación derivado de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.*

Hasta que se produzca la implantación del sistema de planificación para la protección y resiliencia de las entidades críticas regulado en el artículo 7 será de aplicación el sistema de planificación derivado de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, así como de su desarrollo normativo.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Ley 8/2011, de 28 de abril, y cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta ley, sin perjuicio de lo establecido en la disposición transitoria única.

Disposición final primera. *Modificación del texto refundido de la Ley de Puertos del Estado y Marina Mercante, aprobado por el Real Decreto Legislativo 2/2011, de 5 de septiembre.*

Se adiciona un nuevo párrafo u) en artículo 26.1 del texto refundido de la Ley de Puertos del Estado y Marina Mercante, aprobado por el Real Decreto Legislativo 2/2011, de 5 de septiembre, con la siguiente redacción:

«u) Determinar, en coordinación con Puertos del Estado, las personas sobre las que, por tener acceso a zonas de acceso restringido o por desarrollar su actividad en un sector de actividad portuaria sensible para la seguridad, pueda

cve: BOCG-15-A-88-1

solicitarse comprobación de los antecedentes personales al Ministerio del Interior, a través del tratamiento de datos personales al que se refiere disposición adicional quinta de la Ley xxxx, de protección y resiliencia de entidades críticas.»

Disposición final segunda. *Título competencial.*

Esta ley se dicta al amparo de lo previsto en el artículo 149.1. 29.ª, de la Constitución Española, que atribuye al Estado competencia exclusiva en materia de seguridad pública.

Disposición final tercera. *Salvaguarda de la información en el ámbito de la seguridad nacional, la seguridad pública o la defensa nacional.*

El cumplimiento de las obligaciones contenidas en esta ley no implicará el suministro de información o datos cuya divulgación sea contraria a los intereses esenciales de la seguridad nacional, la seguridad pública o la defensa nacional.

Disposición final cuarta. *Competencias en materia de protección civil.*

Lo dispuesto en esta ley se entiende sin perjuicio de lo que establezca la normativa autonómica en materia de protección civil, de acuerdo con lo dispuesto en los correspondientes estatutos de autonomía.

Disposición final quinta. *Incorporación de Derecho de la Unión Europea.*

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

Disposición final sexta. *Desarrollo reglamentario y modificación del anexo.*

1. Se habilita al Gobierno para que dicte las disposiciones necesarias para el desarrollo y aplicación de lo previsto en esta ley.
2. Se habilita a la persona titular del Ministerio del Interior para modificar por orden ministerial el anexo de esta ley.

Disposición final séptima. *Entrada en vigor.*

Esta ley entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

cve: BOCG-15-A-88-1

ANEXO

Sectores, subsectores, organismos responsables y categorías de entidades críticas

Sectores estratégicos	Subsectores estratégicos	Ministerio/Organismo/Entidad	Categorías de entidades
1. Energía.	a) Electricidad.	— M.º para la Transición Ecológica y el Reto Demográfico. — M.º del Interior.	— Las empresas eléctricas tal como se definen en el artículo 2, punto 57, de la Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo, que desempeñan la función de «suministro» tal como se definen en el artículo 2, punto 12, de dicha Directiva.
			— Los gestores de la red de distribución tal como se definen en el artículo 2, punto 29, de la Directiva (UE) 2019/944.
			— Los gestores de la red de transporte tal como se definen en el artículo 2, punto 35, de la Directiva (UE) 2019/944.
			— Los productores tal como se definen en el artículo 2, punto 38, de la Directiva (UE) 2019/944.
			— Los operadores designados para el mercado eléctrico tal como se definen en el artículo 2, punto 8, del Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo.
			— Los participantes en el mercado tal como se definen en el artículo 2, punto 25, del Reglamento (UE) 2019/943 que presten los servicios de agregación, respuesta de demanda o almacenamiento de energía tal como se definen en el artículo 2, puntos 18, 20 y 59, de la Directiva (UE) 2019/944.
	b) Sistemas urbanos de calefacción y de refrigeración.		— Los operadores de sistemas urbanos de calefacción o refrigeración tal como se definen en el artículo 2, punto 19, de la Directiva (UE) 2018/2001 del Parlamento Europeo y del Consejo.
	c) Petróleo y combustibles líquidos.		— Los titulares de instalaciones fijas de almacenamiento y transporte de productos petrolíferos.
			— Los operadores de instalaciones de producción de crudo, instalaciones de refino y tratamiento de crudo, almacenamiento, envasado y transporte.
			— La Entidad Central de Almacenamiento encargada de la gestión de los combustibles líquidos en España (CORES), tal como se definen en el artículo 2, letra f), de la Directiva 2009/119/CE del Consejo.
			— Los operadores al por mayor y distribuidores de productos petrolíferos, incluidos los gases licuados de petróleo y los biocombustibles.
			— Los operadores de plantas de producción de biocombustibles.
	d) Gas natural y biometano.		— Las empresas titulares de concesiones de explotación de yacimientos de gas natural.
			— Las empresas suministradoras tal como se definen en el artículo 2, punto 29, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo.
			— Los gestores de la red de distribución tal como se definen en el artículo 2, punto 20, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo.

cve: BOCG-15-A-88-1

Sectores estratégicos	Subsectores estratégicos	Ministerio/Organismo/Entidad	Categorías de entidades
			— Los gestores de la red de transporte tal como se definen en el artículo 2, punto 18, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo.
			— Los gestores de almacenamientos tal como se definen en el artículo 2, punto 32, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo.
			— Los gestores de la red de GNL tal como se definen en el artículo 2, punto 34, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo.
			— Las empresas de gas natural tal como se definen en el artículo 2, punto 15, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo.
			— Los gestores de las instalaciones de refinado y tratamiento de gas natural.
			— Las empresas productoras de biometano.
	e) Hidrógeno.		— Las empresas de hidrógeno tal y como se definen en el artículo 2, punto 14, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo. — Las empresas suministradoras tal y como se definen en el artículo 2, punto 29, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo. — Los gestores de red de distribución tal y como se definen en el artículo 2, punto 27, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo. — Los gestores de red de transporte tal y como se definen en el artículo 2, punto 26, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo. — Los gestores de almacenamientos tal y como se definen en el artículo 2, punto 6, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo. — Los gestores de terminales de hidrógeno tal y como se definen en el artículo 2, punto 9, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo. — Los gestores de la red de hidrógeno tal y como se definen en el artículo 2, punto 25, de la Directiva (UE) 2024/1788 del Parlamento Europeo y del Consejo.
2. Transporte.	a) Transporte aéreo.	— M.º de Transportes y Movilidad Sostenible o de sus organismos públicos vinculados o dependientes. — M.º del Interior.	— Las compañías aéreas tal como se definen en el artículo 3, punto 4, del Reglamento (CE) 300/2008 utilizadas con fines comerciales.
			— Las entidades gestoras de aeropuertos tal como se definen en el artículo 2, punto 2, de la Directiva 2009/12/CE del Parlamento Europeo y del Consejo, los aeropuertos tal como se definen en el artículo 2, punto 1, de dicha Directiva, incluidos los aeropuertos de la red básica enumerados en el anexo II, sección 2, del Reglamento (UE) 1315/2013 del Parlamento Europeo y del Consejo, y las entidades que explotan instalaciones anexas dentro de los recintos de los aeropuertos.
			— Los proveedores de servicios de navegación aérea, que prestan los servicios y funciones de navegación aérea, tal y como se definen en el artículo 2, puntos 5 y 9 del Reglamento (UE) 2024/2803 del Parlamento Europeo y del Consejo.

cve: BOCG-15-A-88-1

Sectores estratégicos	Subsectores estratégicos	Ministerio/Organismo/Entidad	Categorías de entidades
	b) Transporte por ferrocarril.		— Los administradores de infraestructuras tal como se definen en el artículo 3, punto 2, de la Directiva 2012/34/UE del Parlamento Europeo y del Consejo.
			— Las empresas ferroviarias tal como se definen en el artículo 3, punto 1, de la Directiva 2012/34/ UE, y los explotadores de las instalaciones de servicio tal como se definen en el artículo 3, punto 12, de dicha Directiva.
	c) Transporte marítimo y por vías navegables interiores.		— Compañías de transporte de pasajeros y mercancías por aguas interiores no marítimas, marítimas y costeras, tal como se define compañía para el transporte marítimo por el anexo I del Reglamento (CE) n.° 725/2004 del Parlamento Europeo y del Consejo, excluidos los buques operados por dichas compañías.
			— Entidades gestoras de puertos, tal como se definen estos en el artículo 2, punto 16), del Real Decreto 1617/2007, de 7 de diciembre, incluidas sus instalaciones portuarias, tal como se definen en el artículo 2, punto 11), del Reglamento (CE) n.° 725/2004 del Parlamento Europeo y del Consejo, y entidades que explotan obras y equipos en los puertos.
			— Operadores de servicios de tráfico marítimo (STM), tal como se definen estos servicios en el artículo 3, párrafo o), del Real Decreto 210/2004, de 6 de febrero.
	d) Transporte por carretera.		— Las autoridades viarias tal como se definen en el artículo 2, punto 12, del Reglamento Delegado (UE) 2015/962 de la Comisión responsables del control de la gestión del tráfico, excluidas las entidades públicas para las cuales la gestión del tráfico o la explotación de sistemas de transporte inteligentes es una parte no esencial de su actividad general.
			— Los operadores de sistemas de transporte inteligentes tal como se definen en el artículo 4, punto 1, de la Directiva 2010/40/UE del Parlamento Europeo y del Consejo.
	e) Transporte público.		— Los operadores de servicio público tal como se definen en el artículo 2, letra d), del Reglamento (CE) 1370/2007 del Parlamento Europeo y del Consejo.
3. Banca.		— Banco de España.	— Las entidades de crédito tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 575/2013. — Los sistemas de pagos nacionales.
4. Infraestructuras de los mercados financieros.		— Comisión Nacional del Mercado de Valores.	— Los gestores de los centros de negociación tal como se definen en el artículo 4, punto 24, de la Directiva 2014/65/UE.
			— Las entidades de contrapartida central (ECC) tal como se definen en el artículo 2, punto 1, del Reglamento (UE) 648/2012. — Los depositarios centrales de valores tal y como se definen en el artículo 2, punto 1 del Reglamento (UE) 909/2014.
		— Banco de España.	— Los operadores de sistemas de pago salvo el sistema TARGET-Banco de España (abreviado TARGET-BE), componente español del sistema de grandes pagos denominados en euros TARGET gestionado por el Sistema Europeo de Bancos Centrales, mencionado en el artículo 8.4, de la Ley 41/1999, de 12 de noviembre, sobre sistemas de pagos y de liquidación de valores. — Las entidades procesadoras tal y como se definen en el artículo 2, punto 28 del Reglamento (UE) 2015/751.

cve: BOCG-15-A-88-1

Sectores estratégicos	Subsectores estratégicos	Ministerio/Organismo/Entidad	Categorías de entidades
5. Sanidad.		— M.º de Sanidad. — M.º de Ciencia, Innovación y Universidades. — M.º del Interior. — Ministerio de Industria y Turismo.	— Los prestadores de asistencia sanitaria tal como se definen en el artículo 3, letra g), de la Directiva 2011/24/UE del Parlamento Europeo y del Consejo.
			— Los laboratorios de referencia de la UE a que se refiere el artículo 15 del Reglamento (UE) 2022/2371 del Parlamento Europeo y del Consejo.
			— Las entidades que realizan actividades de investigación y desarrollo sobre los medicamentos tal como se definen en el artículo 1, punto 2, de la Directiva 2001/83/CE del Parlamento Europeo y del Consejo.
			— Las entidades que fabrican productos farmacéuticos de base y especialidades farmacéuticas a que se refiere la sección C, división 21, de la NACE Rev. 2.
			— Las entidades que fabrican productos sanitarios que se consideran indispensables durante una emergencia de salud pública (incluidos en «la lista de productos sanitarios esenciales durante la emergencia de salud pública») en el sentido del artículo 22 del Reglamento (UE) 2022/123 del Parlamento Europeo y del Consejo, así como las que fabrican equipos de protección individual.
			— Las entidades con autorización de distribución a que se refiere el artículo 79 de la Directiva 2001/ 83/CE.
6. Agua.	a) Agua potable.	— M.º para la Transición Ecológica y el Reto Demográfico. — M.º de Sanidad. — M.º del Interior.	— Los suministradores y distribuidores de aguas destinadas al consumo humano tal como se definen en el artículo 2, punto 1, letra a), de la Directiva (UE) 2020/2184 del Parlamento Europeo y del Consejo, excluidos los distribuidores para los cuales la distribución de aguas destinadas al consumo humano solo es una parte no esencial de su actividad general de distribución de otros bienes y productos básicos.
	b) Aguas residuales.		— Las empresas dedicadas a la recogida, la eliminación o el tratamiento de aguas residuales urbanas, aguas residuales domésticas o aguas residuales industriales tal como se definen en el artículo 2, puntos 1, 2 y 3, de la Directiva 91/ 271/CEE del Consejo, excluidas las empresas para las cuales la recogida, la eliminación o el tratamiento de aguas residuales urbanas, aguas residuales domésticas o aguas residuales industriales es una parte no esencial de su actividad general.
7. Infraestructura digital.		— Ministerio del Interior. — Ministerio para la Transformación Digital y la Función Pública.	— Los proveedores de puntos de intercambio de internet tal como se definen en el artículo 6, punto 18, de la Directiva (UE) 2022/2555.
			— Los proveedores de servicios de DNS tal como se definen en el artículo 6, punto 20, de la Directiva (UE) 2022/2555, excluidos los operadores de servidores raíz.
			— Los registros de nombres de dominio de primer nivel tal como se definen en el artículo 6, punto 21, de la Directiva (UE) 2022/2555.
			— Los proveedores de servicios de computación en nube tal como se definen en el artículo 6, punto 30, de la Directiva (UE) 2022/2555.

cve: BOCG-15-A-88-1

Sectores estratégicos	Subsectores estratégicos	Ministerio/Organismo/Entidad	Categorías de entidades
			— Los proveedores de servicios de centro de datos tal como se definen en el artículo 6, punto 31, de la Directiva (UE) 2022/2555.
			— Los proveedores de redes de distribución de contenidos tal como se definen en el artículo 6, punto 32, de la Directiva (UE) 2022/2555.
			— Los prestadores de servicios de confianza tal como se definen en el artículo 3, punto 19, del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo.
			— Los proveedores de redes públicas de comunicaciones electrónicas tal como se definen en el artículo 2, punto 8, de la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo. — Los proveedores de servicios de comunicaciones electrónicas tal como se definen en el artículo 2, punto 4, de la Directiva (UE) 2018/1972, en la medida en que sus servicios estén a disposición del público.
8. Administración pública.		— Presidencia del Gobierno. — Ministerio de la Presidencia, Justicia y Relaciones con las Cortes. — M.º del Interior. — M.º de Defensa. — Centro Nacional de Inteligencia. — M.º de Política Territorial y Memoria Democrática. — M.º para la Transformación Digital y de la Función Pública. — Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. — Ministerio para la Transición Ecológica y el Reto Demográfico. — Ministerio de Hacienda. — Ministerio de Cultura. — Ministerio de Derechos Sociales, Consumo y Agenda 2030.	— Las entidades del sector público institucional.
	Residuos.	— Ministerio para la Transición Ecológica y el Reto Demográfico.	— Empresas dedicadas a la gestión de los residuos, en especial, las destinadas a la gestión de residuos municipales, sanitarios y residuos peligrosos.
9. Espacio.		— M.º de Defensa. — M.º para la Transformación Digital y de la Función Pública. — M.º de Ciencia, Innovación y Universidades. — M.º del Interior. — Ministerio de Transportes y Movilidad Sostenible o sus organismos públicos vinculados o dependientes.	— Los operadores de infraestructuras terrestres, cuya propiedad, gestión y explotación corresponde a la Administración Pública o entidades privadas, que apoyan la prestación de servicios espaciales, excluidos los proveedores de redes públicas de comunicaciones electrónicas tal como se definen en el artículo 2, punto 8, de la Directiva (UE) 2018/1972.
			— Los centros gestores de la información geoespacial e infraestructuras para el geoposicionamiento y la navegación, y del suministro de información para la monitorización y gestión de eventos y peligros geofísicos como los seísmos, tsunamis y volcanes.

cve: BOCG-15-A-88-1

Sectores estratégicos	Subsectores estratégicos	Ministerio/Organismo/Entidad	Categorías de entidades
10. Producción, transformación y distribución de alimentos.		— M.º de Agricultura Pesca y Alimentación. — M.º de Sanidad. — M.º de Industria y Turismo. — M.º del Interior. — Ministerio de Derechos Sociales, Consumo y Agenda 2030.	— Las empresas alimentarias tal como se definen en el artículo 3, punto 2, del Reglamento (CE) n.o 178/2002 del Parlamento Europeo y del Consejo (22) que se dedican exclusivamente a la logística y a la distribución al por mayor y a la producción y transformación industrial a gran escala.
11. Industria nuclear.		— Consejo de Seguridad Nuclear. — M.º para la Transición Ecológica y Reto Demográfico. — M.º del Interior.	— Instalaciones nucleares, instalaciones radiactivas de ciclo combustible y, en el caso de otras instalaciones radiactivas y de transporte de material radiactivo, únicamente aquellos que tienen requerido el establecimiento de un régimen de protección física en cumplimiento de lo establecido en el Real Decreto 1308/2011, de 16 de septiembre, sobre protección física de las instalaciones y los materiales nucleares y de fuentes radiactivas.
12. Instalaciones de investigación.		— M.º de Ciencia, Innovación y Universidades. — M.º para Transición Ecológica y el Reto Demográfico. — M.º del Interior. — Ministerio de Industria y Turismo.	— Laboratorios que por su idiosincrasia dispongan, utilicen o produzcan materiales, sustancias o elementos críticos o peligrosos.
13. Industria química.		— M.º del Interior. — M.º de Industria y Turismo.	— Empresas dedicadas a la producción, almacenamiento y transporte de materiales químicos, mercancías peligrosas.
14. Seguridad privada.		— M.º del Interior.	— Prestación de servicios de seguridad privada relativos a las funciones de seguridad directamente relacionadas con el mantenimiento de los servicios esenciales enumerados en el artículo 2.1 del Real Decreto 524/2002, de 14 de junio, por el que se garantiza la prestación de servicios esenciales en el ámbito de la seguridad privada en situaciones de huelga.
15. Seguros.		— Ministerio de Economía, Comercio y Empresa.	— Entidades aseguradoras y reaseguradoras, tal como se definen en los artículos 2 y 6 de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

cve: BOCG-15-A-88-1