



ANTEPROYECTO DE LEY DE COORDINACIÓN Y GOBERNANZA DE LA CIBERSEGURIDAD

Capítulo I Disposiciones generales

- Artículo 1. *Objeto.*
- Artículo 2. *Definiciones.*
- Artículo 3. *Ámbito de aplicación.*
- Artículo 4. *Entidades esenciales e importantes.*

Capítulo II Marco estratégico e institucional

- Artículo 5. *Estrategia Nacional de Ciberseguridad.*
- Artículo 6. *El Centro Nacional de Ciberseguridad.*
- Artículo 7. *Autoridades de control, punto de contacto único y puntos de contacto sectoriales.*
- Artículo 8. *Marco nacional de gestión de crisis de ciberseguridad.*
- Artículo 9. *Equipos de respuesta a incidentes de ciberseguridad (CSIRT) nacionales de referencia.*
- Artículo 10. *Obligaciones, capacidades técnicas y competencias de los CSIRT nacionales de referencia.*
- Artículo 11. *Divulgación coordinada de las vulnerabilidades.*
- Artículo 12. *Cooperación nacional.*
- Artículo 13. *Cooperación en el ámbito de la Unión Europea.*

Capítulo III Medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación

- Artículo 14. *Gobernanza.*
- Artículo 15. *Medidas generales para la gestión de riesgos de ciberseguridad.*
- Artículo 16. *Responsable de la seguridad de la información.*
- Artículo 17. *Gestión de incidentes de seguridad.*
- Artículo 18. *Obligaciones de notificación.*
- Artículo 19. *Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.*
- Artículo 20. *Información sobre incidentes.*
- Artículo 21. *Actuaciones ante incidentes con carácter presuntamente delictivo.*
- Artículo 22. *Protección del notificante.*
- Artículo 23. *Obligaciones de información y colaboración.*
- Artículo 24. *Cooperación en lo relativo a los incidentes que afecten a datos personales.*
- Artículo 25. *Autorización para la cesión de datos personales.*



Capítulo IV **Registros de entidades de naturaleza transfronteriza**

Artículo 26. *Registro de proveedores de servicios e infraestructuras digitales.*

Artículo 27. *Base de datos sobre el registro de nombres de dominio.*

Capítulo V **Intercambio de Información**

Artículo 28. *Mecanismos de intercambio de información sobre ciberseguridad.*

Artículo 29. *Notificación voluntaria de información pertinente.*

Capítulo VI **Supervisión y Ejecución**

Artículo 30. *Aspectos generales relativos a la supervisión de entidades esenciales e importantes.*

Artículo 31. *Medidas de supervisión y ejecución relativas a entidades esenciales.*

Artículo 32. *Medidas de supervisión y ejecución en relación con entidades importantes.*

Artículo 33. *Utilización de esquemas europeos de certificación de la ciberseguridad.*

Artículo 34. *Cooperación transfronteriza.*

Capítulo VII **Régimen sancionador**

Sección 1.ª Reglas generales.

Artículo 35. *Sujetos responsables.*

Artículo 36. *Competencia sancionadora.*

Artículo 37. *Criterios de graduación de las sanciones.*

Sección 2.ª Infracciones y sanciones

Artículo 38. *Clasificación de las infracciones.*

Artículo 39. *Infracciones muy graves.*

Artículo 40. *Infracciones graves.*

Artículo 41. *Infracciones leves.*

Artículo 42. *Sanciones.*

Artículo 43. *Infracciones de las Administraciones Públicas.*

Sección 3.ª Procedimiento sancionador

Artículo 44. *Régimen jurídico.*



Artículo 45. *Concurrencia de infracciones.*

Artículo 46. Subordinación del procedimiento administrativo sancionador respecto del penal.

Artículo 47. *Medidas provisionales.*

Artículo 48. *Caducidad del procedimiento.*

Artículo 49. Prescripción de las infracciones.

Artículo 50. Prescripción de las sanciones.

Disposición adicional primera. *Creación del Centro Nacional de Ciberseguridad.*

Disposición adicional segunda. *Régimen específico del Banco de España.*

Disposición adicional tercera. *Información sobre incidentes en el sistema financiero.*

Disposición adicional cuarta. Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

Disposición adicional quinta. *Base de datos de incidencias de seguridad que revistan carácter de delito*

Disposición adicional sexta. *Salvaguarda de intereses y funciones estatales esenciales*

Disposición adicional séptima. *Representación en el Centro Europeo de Competencia Industrial.*

Disposición adicional octava. *Autoridad Nacional de Certificación.*

Disposición transitoria primera. *Obligaciones de comunicación.*

Disposición transitoria segunda. *Registro de entidades.*

Disposición transitoria tercera. *Régimen transitorio.*

Disposición derogatoria única. *Derogación normativa.*

Disposición final primera. *Título competencial.*

Disposición final segunda. *Modificación de la Ley 5/2014, de 4 de abril, de Seguridad Privada.*

Disposición final tercera. *Desarrollo reglamentario.*

Disposición final cuarta. *Incorporación al derecho de la Unión Europea*

Disposición final quinta. *Entrada en vigor.*



EXPOSICIÓN DE MOTIVOS

I

El uso cotidiano de las redes y sistemas de información se ha convertido en un aspecto crucial para el desarrollo de las actividades sociales y económicas gracias a la velocidad de la transformación digital y la creciente interconexión de la sociedad. Esta positiva evolución ha supuesto, sin embargo, una expansión del panorama de las ciberamenazas, con la consiguiente aparición de nuevos desafíos y riesgos que requieren respuestas adaptadas, coordinadas e innovadoras. El número, la magnitud, la sofisticación, la frecuencia y los efectos de los incidentes de naturaleza cibernética representan una grave amenaza para el funcionamiento de las redes y sistemas de información, que pueden llegar a perturbar las actividades económicas, mermar la confianza de los usuarios y ocasionar grandes daños a la economía, la sociedad y la seguridad nacional, y requieren de un esfuerzo permanente para combatirlos. Prueba de ello es que la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, impone a los operadores de redes públicas de comunicaciones electrónicas y de servicios de comunicaciones electrónicas disponibles al público la obligación de gestionar adecuadamente los riesgos de seguridad que puedan afectar a sus redes y servicios a fin de garantizar un adecuado nivel de seguridad y evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en otras redes y servicios. Todo ello hace que la mejora de la preparación en materia de ciberseguridad resulte más esencial que nunca.

El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, transpuso a nuestro ordenamiento la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, cuyo objetivo era el desarrollo de las capacidades en materia de ciberseguridad, y reducir las amenazas para las redes y sistemas de información utilizados para prestar servicios esenciales en sectores fundamentales, garantizando la continuidad de dichos servicios en caso de incidentes, al tiempo que también propiciaba la cooperación en esta materia a nivel de la Unión Europea. A pesar de estos logros, la revisión de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, puso de manifiesto algunas deficiencias inherentes que le impedían abordar eficazmente los retos actuales y emergentes en el ámbito de la ciberseguridad, afectando, en particular, a la prestación transfronteriza de servicios y al nivel de ciberresiliencia entre distintos Estados miembros debido a la aplicación de medidas dispares.

Con el fin de superar esas deficiencias, se ha aprobado 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) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148. Esta Directiva, que es objeto de transposición por esta norma, tiene como objetivos: regular un marco institucional, mejorar la



coordinación entre autoridades competentes y los órganos de cooperación relevantes en el ámbito comunitario, ofrecer una cobertura completa de los sectores y servicios de vital importancia para las actividades sociales y económicas fundamentales dentro del mercado interior, y garantizar la seguridad jurídica en lo que se refiere a las medidas para la gestión de riesgos de ciberseguridad y las obligaciones de notificación.

En particular, la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, establece un criterio uniforme para determinar qué entidades están incluidas en su ámbito de aplicación de la norma, y por lo tanto, deben cumplir las medidas para la gestión de riesgos de ciberseguridad. A tal fin, las entidades se clasifican en dos categorías: entidades esenciales y entidades importantes, en función del grado de criticidad de sus sectores o, del tipo de servicio que prestan, así como de su tamaño. Al mismo tiempo, dada la intensificación y sofisticación de las ciberamenazas en el mundo actual, se garantiza que las entidades excluidas del ámbito de aplicación de la presente norma alcancen un elevado nivel de ciberseguridad, apoyando la aplicación de medidas equivalentes de gestión de riesgos de ciberseguridad que reflejen el carácter sensible de dichas entidades, manteniendo un adecuado nivel de cooperación y comunicación entre las respectivas autoridades competentes.

Asimismo, en vista de las interrelaciones que existen entre la ciberseguridad y la seguridad física de las entidades, debe garantizarse un enfoque coherente entre las disposiciones por las que se transponen la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, y 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. Para ello, se impone la necesidad de que la estrategia nacional de ciberseguridad establezca un marco de actuación para mejorar la coordinación entre las autoridades competentes en el contexto del intercambio de información tanto sobre los riesgos, ciberamenazas e incidentes relacionados con la ciberseguridad, como sobre los riesgos, amenazas e incidentes no relacionados con la ciberseguridad, y sobre el ejercicio de las tareas de supervisión. En este sentido, por una parte, las entidades que hayan sido identificadas como críticas en el contexto de la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, deben también ser consideradas entidades esenciales a los efectos de esta ley; y por otra, las obligaciones impuestas a las entidades pertenecientes al sector de las infraestructuras digitales deben abordar de manera exhaustiva, como parte de sus medidas para la gestión de los riesgos de ciberseguridad y obligaciones de notificación, la seguridad física de las redes y sistemas de información. Dado que esas cuestiones entran en el ámbito de aplicación de esta ley, las obligaciones establecidas a este respecto en la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, no se aplican a dichas entidades.

Por otro lado, el preámbulo de la Directiva objeto de transposición contempla la posibilidad de que se den crisis de ciberseguridad con una importante dimensión exterior o de política común de seguridad y defensa, aunque no aborda materias relativas a Defensa Nacional,



que por ser competencia exclusiva de los Estados miembros, deben dejarse a la regulación nacional, sin renunciar por ello a una estrategia común. En este sentido, es importante señalar que la Estrategia Europea de Ciberseguridad de 2020 incluye, entre las medidas de su segunda línea de acción, las orientadas al impulso de las capacidades de Ciberdefensa, y entre ellas la consolidación del ciberespacio como dominio de las operaciones militares y el establecimiento de la Red de CERT Militares (Military Cert-Network), de la que ya forma parte el ESPDEF-CERT del Mando Conjunto del Ciberespacio, para contribuir de forma significativa a la cooperación entre los Estados miembros de la UE. La necesidad de impulsar esta misma línea de colaboración se mantiene en la Política de Ciberdefensa de la Unión Europea de 2022.

II

La Unión Internacional de Telecomunicaciones define la ciberseguridad como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. A su vez, el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»), incluye en el concepto de ciberseguridad todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas. Partiendo del carácter transversal e interconectado de las tecnologías de la información y las comunicaciones y de la conceptualización de la ciberseguridad como conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan estos sistemas interconectados, no es un concepto o materia reconducible a un único título competencial.

De este modo, la ciberseguridad mantiene una indudable conexión con la seguridad nacional. En este sentido, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, incluye expresamente la ciberseguridad como un ámbito de especial interés para la seguridad nacional, que requiere una atención específica, así como lo hace la Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad, atención que se materializa por medio de la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional, como marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada, y en la participación de la ciudadanía, en el que se sientan las prioridades, objetivos y medidas adecuadas para alcanzar y mantener un elevado nivel de seguridad de



las redes y sistemas de información, y en cuyo ámbito, se aprobó por Acuerdo de Consejo de Ministros de 29 de marzo de 2022, el vigente Plan Nacional de Ciberseguridad.

Asimismo, en atención al carácter de la Defensa Nacional como un componente fundamental de la Seguridad Nacional y en cumplimiento de las obligaciones que la Ley 36/2015 impone a las Administraciones Públicas con competencias en los ámbitos de especial interés de la Seguridad Nacional, se deben articular los mecanismos de apoyo a operadores con incidencia en la Defensa Nacional y de coordinación e intercambio de información, especialmente en relación con los sistemas de vigilancia y alerta ante posibles riesgos y amenazas que afecten a ésta y a las Fuerzas Armadas.

Asimismo, a partir de su caracterización como conjunto de mecanismos dirigidos a la protección de las infraestructuras tecnológicas y de la información digital que albergan, se infiere que, en tanto que dedicada a la seguridad de las tecnologías de la información, la ciberseguridad presenta un componente tuitivo que se proyecta específicamente sobre el concreto ámbito de la protección de las redes y sistemas de información que utilizan los ciudadanos, empresas y administraciones públicas. Por tanto, como sinónimo de la seguridad en la red, la ciberseguridad es una actividad que se integra en la seguridad pública, así como en las telecomunicaciones. La seguridad pública es una competencia exclusiva del Estado, y es doctrina consolidada del Tribunal Constitucional que ésta solamente se encuentra limitada por la atribución a las Comunidades Autónomas de facultades relativas a la creación de las policías autonómicas, como forma de participación de éstas en el ejercicio de aquella competencia. Procede recordar, no obstante, que la materia de seguridad pública se proyecta más allá de las funciones propias de las fuerzas y cuerpos de seguridad, de tal suerte que éstas constituyen solo una parte de la materia más amplia de la seguridad pública. En tal sentido, además de los servicios policiales que en todo caso se encuentran reservados a las fuerzas y cuerpos de seguridad del Estado, corresponden al Estado las restantes potestades o facultades administrativas que, siendo relevantes para la seguridad pública, como son las relativas al ámbito de la ciberseguridad, no sean sin embargo propias ni inherentes de las funciones o servicios policiales.

Igualmente, incide en esta materia la competencia exclusiva estatal en materia de telecomunicaciones y de régimen general de comunicaciones que, desde una perspectiva global, integra tanto los aspectos técnicos como las competencias normativas sobre la misma, y también comporta la atribución de las competencias de supervisión y ejecución necesarias para garantizar la continuidad de los servicios y configurar un sistema materialmente unitario y homogéneo en todo el territorio nacional, necesario no sólo para el desarrollo del sector sino para la seguridad y garantía de los derechos de los ciudadanos.

III

Esta ley consta de cincuenta artículos, estructurados en siete capítulos, así como de ocho disposiciones adicionales, tres disposiciones transitorias, una disposición derogatoria y cinco disposiciones finales.



En el capítulo I, se regula el objeto y el ámbito de aplicación objetivo y subjetivo de la ley y se definen los criterios de identificación de las entidades esenciales e importantes. Se incluyen las principales definiciones que se deben aplicar y conocer, de forma que todos los agentes implicados en su interpretación tengan conocimiento de los elementos básicos para encontrar el sentido y alcance de cada precepto.

El capítulo II establece el marco nacional, estratégico e institucional, para la seguridad de las redes y sistemas de información, con objeto de alcanzar y mantener un elevado nivel de ciberseguridad. A tal efecto, se determinan los contenidos mínimos que deben ser abordados por la estrategia nacional de ciberseguridad. A destacar como la principal novedad y el aspecto más significativo de este capítulo, se contempla la existencia del Centro Nacional de Ciberseguridad, que, superando la actual dispersión competencial en materia de ciberseguridad, se constituye en autoridad nacional competente única en la materia para la dirección, impulso y coordinación de todas las actividades previstas en esta ley, como punto de contacto único para garantizar la cooperación intersectorial y transfronteriza con otras autoridades competentes, así como autoridad nacional de gestión de crisis de ciberseguridad. También se establecen medidas para garantizar una cooperación efectiva, eficiente y segura en el ámbito de la Unión Europea.

En el capítulo III se regulan las medidas para la gestión de riesgos de ciberseguridad y las obligaciones de notificación. Se contempla en esta parte la realización de una evaluación individualizada del riesgo por parte de las distintas entidades, y se detallan las actuaciones a llevar a cabo por éstas para garantizar y elevar sus niveles de seguridad de las redes y sistemas de información y prevenir el riesgo de incidentes, así como la obligación de notificar los incidentes significativos que se produzcan en su operativa o en la prestación de sus servicios. Para dar cumplimiento a las obligaciones de notificación se pondrá a disposición de todos los actores involucrados la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, que permitirá el intercambio de información técnica y el seguimiento de incidentes. Asimismo, se recoge la figura del responsable de la seguridad de la información, como persona u órgano designado por las entidades esenciales e importantes, encargado de las funciones de punto de contacto y de la coordinación técnica en las materias objeto de esta ley.

Por su parte, lo más destacado del capítulo IV consiste en la imposición de la obligación de la elaboración y actualización periódica de registros de carácter transfronterizo, en concreto de proveedores de servicio e infraestructuras digitales, así como de entidades que prestan servicios de registro de nombres de dominio, con objeto de garantizar una visión clara de las entidades incluidas en el ámbito de aplicación de la presente norma. Al mismo tiempo, el capítulo V se consagra al intercambio voluntario entre entidades de información relevante con el objetivo de reforzar el nivel de ciberseguridad y prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión, así como a la notificación a la autoridad de control, a través de los CSIRT nacionales de referencia, de aquellos incidentes para los que no se establezca una obligación de notificación.



El capítulo VI está dedicado a la regulación de las funciones de supervisión y ejecución sobre las entidades esenciales e importantes, así como a la cooperación transfronteriza; y el capítulo VII al desarrollo de las potestades disciplinarias, en cumplimiento de las previsiones del artículo 36 de la Directiva, a fin de garantizar el cumplimiento efectivo de las obligaciones contempladas en la presente ley. 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 ley también incorpora siete disposiciones adicionales y tres transitorias. Entre las primeras destaca la creación del Centro Nacional de Ciberseguridad, con el rango, carácter y estructura administrativa que se determine, con el fin de dar cumplimiento a las disposiciones de esta ley para hacer posible alcanzar un elevado nivel de ciberseguridad nacional en todos sus ámbitos. Igualmente, para la gestión, seguimiento y resolución de incidentes de ciberseguridad que afecten a entidades esenciales e importantes, que puedan ser presuntamente delictivos, se contempla el tratamiento denominado base de datos de incidencias de seguridad que revistan carácter de delito.

Las disposiciones transitorias trasladan a la norma las obligaciones de comunicación y notificación a la Comisión de los distintos hitos e informaciones relacionados con la implementación de las disposiciones de la Directiva y establecen el régimen competencial vigente hasta que tenga lugar el desarrollo institucional previsto en esta ley para dar cumplimiento a las obligaciones recogidas en la misma.

Por último, en las disposiciones finales se modifica la Ley 5/2014, de 4 de abril, de Seguridad Privada para incluir al personal que realice tareas de ciberseguridad como personal acreditado.

Asimismo, se señala que por medio de esta norma se incorpora al Derecho español 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) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) y, en línea con lo que hace la propia Directiva que se transpone, por medio de la disposición derogatoria se derogan, a su vez, las normas nacionales a través de las que en su día se transpuso la Directiva (UE) 2016/1148.

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) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2), exige el desarrollo de una norma con rango legal. El principio de necesidad está estrechamente vinculado al de seguridad jurídica, en cuanto a la materia objeto de regulación, puesto que la transposición de la citada Directiva se lleva a cabo mediante una ley. Por lo que la tramitación e integración en el ordenamiento jurídico goza de las garantías que amparan las normas de esta naturaleza.

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, de 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.

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

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

Por último, la presente ley se dicta al amparo de lo previsto en el artículo 149.1. 4ª, 21.ª y 29.ª de la Constitución Española, que atribuyen respectivamente al Estado competencia exclusiva en materia de Defensa, régimen general de telecomunicaciones y de seguridad pública.



Capítulo I Disposiciones generales

Artículo 1. *Objeto.*

Esta ley tiene por objeto establecer medidas para alcanzar un elevado nivel común de ciberseguridad en España y contribuir a la ciberseguridad de la Unión Europea.

A tal fin, establece:

- a) Obligaciones que requieren la adopción de una estrategia nacional de ciberseguridad y la designación o establecimiento de autoridades competentes, autoridades de control, autoridad de gestión de crisis de ciberseguridad, punto de contacto único sobre ciberseguridad (en lo sucesivo, “punto de contacto único”) y equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés);
- b) Medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades reguladas en esta ley cuyo tipo se enmarca en los anexos I o II; así como para las entidades identificadas como críticas con arreglo a la Ley XXXX (Directiva (UE) 2022/2557);
- c) Normas y obligaciones relativas al intercambio de información sobre ciberseguridad;
- d) Obligaciones de supervisión y ejecución.

Artículo 2. *Definiciones.*

A los efectos de esta ley se entenderá por:

- a) redes y sistemas de información:
 - i. Un red de comunicaciones electrónicas, entendiéndose por tal los sistemas de transmisión, se basen o no en una infraestructura permanente o en una capacidad de administración centralizada, y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos, incluidos los elementos de red que no son activos, que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes fijas (de conmutación de circuitos y de paquetes, incluido internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada;



- ii. Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, conforme a un programa, el tratamiento automático de datos digitales, o
 - iii. Los datos digitales almacenados, tratados, recuperados o transmitidos mediante elementos contemplados en las letras i) e ii) para su funcionamiento, utilización, protección y mantenimiento.
- b) seguridad de las redes y sistemas de información: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, cualquier hecho que pueda comprometer la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos por tales redes y sistemas de información o accesibles a través de ellos;
- c) ciberseguridad: todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas;
- d) estrategia nacional de ciberseguridad: marco coherente de un Estado miembro que establece prioridades y objetivos estratégicos en el ámbito de la ciberseguridad y la gobernanza para alcanzarlos en dicho Estado miembro;
- e) cuasiincidente o incidente sin impacto: un hecho que habría podido comprometer la disponibilidad, autenticidad, integridad confidencialidad, o trazabilidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por redes y sistemas de información o accesibles a través de ellos, pero cuya materialización completa se previno de manera satisfactoria o que no llegó a materializarse;
- f) incidente: todo hecho que comprometa la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por redes y sistemas de información o accesibles a través de ellos;
- g) incidente significativo: se considerará tal, si
 - i. ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada;
 - ii. ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables.
- h) incidente de ciberseguridad a gran escala: un incidente que cause perturbaciones que superen la capacidad de un Estado miembro para responder a él o que afecte significativamente por lo menos a dos Estados miembros;
- i) gestión de incidentes: conjunto de medidas y procedimientos destinados a prevenir, detectar, analizar y limitar un incidente o responder ante este y recuperarse de él;
- j) ciberamenaza: una ciberamenaza tal como se define en el artículo 2, punto 8, del Reglamento (UE) 2019/881;
- k) ciberamenaza significativa: una ciberamenaza que, basándose en sus características técnicas, cabe suponer que tiene el potencial de provocar repercusiones graves en las redes y sistemas de información de una entidad o para



los usuarios de los servicios de la entidad causando perjuicios materiales o inmateriales considerables;

- l) 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;
- m) vulnerabilidad: deficiencia, susceptibilidad o fallo de productos de TIC o servicios de TIC que puede ser aprovechado por una ciberamenaza;
- n) sistema de nombres de dominio (DNS): un sistema de nombres distribuido jerárquicamente que posibilita la identificación de servicios y recursos de internet, permitiendo a los dispositivos de los usuarios finales utilizar servicios de enrutamiento y conectividad de internet para acceder a dichos servicios y recursos;
- a) proveedor de servicios de DNS: una entidad que presta servicios a disposición pública de resolución recursiva de nombres de dominio para usuarios finales de internet, o servicios de resolución autoritativa de nombres de dominio para uso por terceros, con excepción de los servidores raíz; o servicios de resolución autoritativa de nombres de dominio para uso por terceros, con excepción de los servidores raíz;
- o) registro de nombres de dominio de primer nivel: una entidad en la que se ha delegado un dominio de primer nivel específico y que es responsable de administrar dicho dominio, incluido el registro de nombres de dominio en el dominio de primer nivel y el funcionamiento técnico del dominio de primer nivel, en particular la explotación de sus servidores de nombre, el mantenimiento de sus bases de datos y la distribución de los archivos de zona del dominio de primer nivel entre los servidores de nombre, independientemente de que cualquiera de esas operaciones sea realizada por la entidad o se haya externalizado, pero excluyendo las situaciones en las que los nombres de dominio de primer nivel sean utilizados por un registro únicamente para su propio uso;
- p) entidad que presta servicios de registro de nombres de dominio: un registrador o un agente que actúe en nombre de los registradores, como un proveedor o revendedor de servicios de registro de privacidad o representación;
- q) mercado en línea: un servicio que emplea programas (“software”), incluidos un sitio web, parte de un sitio web o una aplicación, operado por el comerciante o por cuenta de este, que permite a los consumidores celebrar contratos a distancia con otros comerciantes o consumidores;
- r) motor de búsqueda en línea: un servicio digital que permite a los usuarios introducir consultas para hacer búsquedas de, en principio, todos los sitios web, o de sitios web en un idioma concreto, mediante una consulta sobre un tema cualquiera en forma de palabra clave, consulta oral, frase u otro tipo de entrada, y que en respuesta muestra resultados en cualquier formato en los que puede encontrarse información relacionada con el contenido solicitado;
- s) servicio de computación en nube: un servicio digital que hace posible la administración bajo demanda y el acceso remoto amplio a un conjunto modulable y elástico de recursos informáticos que se pueden compartir, también cuando dichos recursos están distribuidos entre varias ubicaciones;



- t) servicio de centro de datos: un servicio que engloba las estructuras, o agrupaciones de estructuras, dedicadas al alojamiento, la interconexión y la explotación centralizados de las tecnologías de la información y los equipos de red que proporcionan servicios de almacenamiento, tratamiento y transporte de datos, junto con todas las instalaciones e infraestructuras necesarias para la distribución de la energía y el control ambiental;
- u) red de distribución de contenidos: una red de servidores distribuidos geográficamente a efectos de garantizar una elevada disponibilidad, accesibilidad o distribución rápida de contenidos y servicios digitales a los usuarios de internet en nombre de los proveedores de contenidos y servicios;
- v) plataforma de servicios de redes sociales: una plataforma que permite que los usuarios finales se conecten, compartan, descubran y se comuniquen entre sí a través de múltiples dispositivos, en particular, mediante chats, publicaciones, vídeos y recomendaciones;
- w) proveedor de servicios gestionados: una entidad que presta servicios relacionados con la instalación, la gestión, la explotación o el mantenimiento de productos, redes, infraestructuras o aplicaciones de TIC o cualesquiera otras redes y sistemas de información, a través de la asistencia o la administración activa, en las instalaciones de los clientes o a distancia;
- x) proveedor de servicios de seguridad gestionados: un proveedor de servicios gestionados que lleva a cabo actividades relativas a la gestión de riesgos de ciberseguridad o presta asistencia para ello;
- y) Medidas generales para la gestión de riesgos de ciberseguridad: conjunto de medidas de carácter técnico, operativo, y organizativo que utiliza una entidad en sus operaciones o en la prestación de sus servicios, que tienen por objeto gestionar los riesgos para la seguridad de las redes y sistemas de información, y prevenir o minimizar las repercusiones de los incidentes en sus usuarios y en otros servicios.
- z) Entidades u operadores con Incidencia en la Defensa Nacional: Aquellas entidades esenciales o importantes, de cualquier sector, proveedoras de bienes o servicios necesarios para el funcionamiento del Ministerio de Defensa y en especial para el cumplimiento de las misiones de las Fuerzas Armadas, que se establezcan de conformidad con los artículos 3 y 4 de esta Ley.
- aa) Perfil de cumplimiento específico: conjunto de medidas de seguridad, comprendidas o no en el anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el Centro Criptológico Nacional.
- bb) Auditoría de la seguridad: es un proceso sistemático, independiente y documentado que persigue la obtención de evidencias y su evaluación objetivas para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios.



- cc) Red europea de Centros de Operaciones de Ciberseguridad (En inglés ENSOC): infraestructura tecnológica europea formada por un conjunto de centros nacionales pertenecientes a los Estados Miembros, organizada en torno a un consorcio europeo, y cuyo objetivo es establecer una plataforma de Centro de Operaciones de Seguridad (SOC) transfronteriza para mejorar la detección y prevención de amenazas cibernéticas, proporcionar advertencias oportunas a las autoridades y partes interesadas y, en su consecuencia, reforzando el Sistema Europeo de Alerta de Ciberseguridad (Cybersecurity Alert System).

Artículo 3. *Ámbito de aplicación.*

1. Se aplicará a las entidades públicas o privadas que tengan su residencia fiscal en España y que se encuentren dentro de los sectores de alta criticidad y otros sectores críticos recogidos en los Anexos I y II, cuando tengan la consideración de medianas o grandes empresas porque cuentan con 50 o más trabajadores, y tengan un volumen de negocios anual o un balance general anual que supera los 10 millones de euros.

2. Independientemente de su tamaño, se aplicará a las entidades comprendidas en los Anexos I o II, en los siguientes supuestos:

- a) Los servicios son prestados por:
 - i. proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público;
 - ii. prestadores de servicios de confianza;
 - iii. registros de nombres de dominio de primer nivel y proveedores de servicios de sistema de nombres de dominio;
- b) La entidad sea el único proveedor en España de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas;
- c) Una perturbación del servicio prestado por la entidad pudiera tener repercusiones significativas sobre la seguridad nacional, la seguridad pública, el orden público, la salud pública, la actividad económica, o la prestación de servicios públicos
- d) Una perturbación del servicio prestado por la entidad pudiera inducir riesgos sistémicos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo;
- e) La entidad pertenezca al sector público de acuerdo con el artículo 2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- f) Entidades críticas, de conformidad con la normativa aplicable a las medidas para la protección de infraestructuras críticas.
- g) Universidades y Centros de Investigación, en asuntos o proyectos de investigación relacionados con los sectores de alta criticidad y otros sectores críticos.
- h) Empresas en las que el 25 % o más de su capital o de sus derechos de voto, estén controlados, directa o indirectamente, por uno o más organismos o administraciones pertenecientes al sector público, y que sean así identificadas por la autoridad de control, salvo que pueda ser considerada una empresa vinculada.



- i) Cualquier otra entidad que la autoridad de control identifique como entidad esencial o importante aplicando los criterios del presente artículo, mediante resolución motivada.

3. También serán de aplicación las disposiciones de esta ley a las entidades que, teniendo su residencia o domicilio en otro Estado de la Unión Europea, ofrezcan sus servicios o desarrollen sus competencias a través de un establecimiento permanente situado en España, de acuerdo con los criterios siguientes:

- a) Los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público, cuando presten servicios en España.
- b) Los proveedores de servicios e infraestructura tecnológica recogidos en el artículo 26.1, cuando tengan su establecimiento principal en España.

Se considerará que tienen su establecimiento principal en España cuando:

- i) las decisiones relativas a las medidas para la gestión de riesgos de ciberseguridad se adopten predominantemente en territorio español.
- ii) En caso de que no pueda determinarse dónde se adoptan tales decisiones, o en caso de que se realice fuera de la Unión Europea, cuando se desarrollen en España las operaciones de ciberseguridad.
- iii) En caso de que no se pueda determinar en qué Estado de la Unión Europea en que las realizan, cuando la entidad tenga en España el establecimiento con mayor número de trabajadores en la Unión Europea.

4. El Centro Nacional de Ciberseguridad implementará los procedimientos necesarios para identificar qué entidades se encuentran recogidas en los apartados anteriores, con ayuda de las autoridades de control y puntos de contacto sectoriales.

5. Se excluyen de su ámbito de aplicación:

- a) Las entidades de la Administración pública que realicen actividades en los ámbitos de la seguridad nacional, la defensa nacional, o la seguridad pública, incluyendo la prevención, investigación, detección y enjuiciamiento de infracciones penales, salvo en aquellas actividades en las que actúen como prestadores de servicios de confianza disponibles para terceros.
- b) El Instituto de Crédito Oficial.



6. No se aplicarán a las entidades financieras comprendidas en el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de , 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 y (UE) 2016/1011 las disposiciones de la esta ley relativas a las obligaciones de gestión de los riesgos de ciberseguridad y de notificación, y a la supervisión y ejecución. Tampoco resultarán aplicables a este tipo de entidades lo dispuesto en el artículo 33, ni las disposiciones contenidas en el capítulo VII relativo al régimen sancionador, sin perjuicio de la obligación de colaboración e intercambio de información del sector financiero con las autoridades de control y del carácter complementario de esta ley con respecto a las disposiciones del Reglamento anteriormente citado.

Artículo 4. *Entidades esenciales e importantes.*

1. Se consideran entidades esenciales:

- a) Las entidades pertenecientes a los sectores recogidos en el Anexo I, que se consideren grandes empresas por emplear 250 o más trabajadores y tener un volumen de negocio anual superior a 50 millones de euros o un balance general anual superior a 43 millones de euros.
- b) Los prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel, así como proveedores de servicios de DNS, independientemente de su tamaño.
- c) Los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles para el público que sean consideradas medianas empresas, por emplear a 50 o más trabajadores sin superar la cifra de 250, y tener un volumen anual de negocios o un balance general anual de más de 10 millones de euros y no superior a 50 millones de euros.
- d) Entidades de la Administración General del Estado y de las Administraciones de las Comunidades Autónomas, de acuerdo con el artículo 2 de la Ley 40/2015, de 1 de octubre diputaciones provinciales, cabildos y consejos insulares y municipios de gran población definidos en el Título X de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. Serán considerados esenciales las entidades del sector público institucional de todas las anteriores, salvo resolución motivada en contrario de la autoridad de control, o que así se disponga reglamentariamente.
- e) Cualquier otra entidad de los sectores recogidos en los Anexos I o II de esta Ley, que las autoridades de control identifiquen como entidad esencial en virtud del artículo 3, apartado 2, letras b) y c).



- f) Entidades identificadas como entidades críticas con arreglo a la Ley xxxx.
- g) Las entidades identificadas como operadores de servicios esenciales antes del 16 de enero de 2023 en virtud del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. Son entidades importantes todas las entidades pertenecientes a los sectores recogidos en los citados Anexos I o II que no puedan considerarse entidades esenciales con arreglo al apartado 1 del presente artículo. Ello incluye las entidades que las autoridades de control identifiquen como entidad importante en virtud del artículo 3, apartado 2, letras b), c), d), e) y f), y, en todo caso, a los municipios que, no siendo municipios de gran población, su población sea superior a 20.000 habitantes, y las entidades de su sector público institucional.

3. El Centro Nacional de Ciberseguridad, sobre la base de la información suministrada por las autoridades de control, elaborará una lista de entidades esenciales e importantes. Esta lista se revisará con regularidad, al menos cada dos años, y, si procede, se actualizará.

4. Para la elaboración de la lista, las entidades recogidas en el apartado anterior deberán evaluar su inclusión en las categorías de entidades esenciales e importantes y en su caso, remitir a las autoridades de control en el plazo máximo de tres meses desde la adquisición de su condición de tales, al menos, la siguiente información:

- a) El nombre de la entidad.
- b) La dirección y los datos de contacto actualizados, incluidas las direcciones de correo electrónico, los rangos de IP y los números de teléfono, incluyendo en su caso los datos de contacto del responsable de la seguridad de la información de la entidad.
- c) En su caso, el sector y el subsector al que pertenecen, de acuerdo con los Anexos I y II.
- d) En su caso, una lista de los Estados miembros de la Unión Europea en los que prestan servicios comprendidos en el ámbito de aplicación de Directiva (UE) 2022/2555, del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Las entidades a que se refiere el apartado 3 deberán notificar a las autoridades de control, cualquier cambio en la información que hayan remitido a la mayor brevedad y, en cualquier caso, en el plazo de dos semanas desde la desde la fecha en que se produjo el cambio.

Reglamentariamente se podrán establecer los mecanismos para que las entidades den cumplimiento a las obligaciones de este apartado registrándose ellas mismas.



5. Las autoridades de control serán responsables de identificar, a propuesta del Jefe del Estado Mayor de la Defensa, las entidades consideradas entidades con incidencia en la defensa nacional, y comunicarán a las mismas su alta o baja como tales.

En el caso de entidades críticas, conforme a la ley xxxx, por la que se transpone la Directiva (UE) 2022/2557, la identificación requerirá el informe previo de la Oficina de Coordinación de Ciberseguridad.

En el ámbito de esta Ley, el Jefe del Estado Mayor de la Defensa, a través del Mando Conjunto del Ciberespacio (MCCE), será responsable de coordinar, con el Centro Nacional de Ciberseguridad y con las autoridades de control o, cuando se trate de entidades críticas, con las autoridades designadas conforme a la ley xxxx, por la que se transpone la Directiva (UE) 2022/2557, los apoyos prestados a entidades con incidencia en la Defensa Nacional.

6. El ESPDEF-CERT del Mando Conjunto del Ciberespacio será responsable del registro de las entidades con incidencia en la defensa nacional designadas, e informará de su identidad al CSIRT nacional de referencia, así como a las autoridades competentes designadas conforme a la ley xxxx, por la que se transpone la Directiva (UE) 2022/2557, del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, en el caso de que se trate de entidades críticas.

7. Cuando una normativa nacional o comunitaria establezca para un sector obligaciones de seguridad de las redes y sistemas de información o de notificación de incidentes que tengan efectos, al menos, equivalentes a los de las obligaciones previstas en esta ley, prevalecerán aquellos requisitos y los mecanismos de supervisión correspondientes.

Capítulo II **Marco estratégico e institucional**

Artículo 5. Estrategia Nacional de Ciberseguridad.

1. La Estrategia Nacional de Ciberseguridad establecerá los objetivos estratégicos, los recursos necesarios y las medidas políticas y normativas adecuadas para alcanzar y mantener un nivel elevado de ciberseguridad. Su contenido será coherente con la Estrategia de Seguridad Nacional.

2. La Estrategia Nacional de Ciberseguridad deberá establecer, entre otras, las siguientes cuestiones:

a) Sus objetivos y prioridades, en particular, los sectores recogidos en los anexos I y II, y la relación de las autoridades y partes interesadas que participan en su ejecución.



- b) El marco de gobernanza para lograr los objetivos y prioridades mencionados en la letra a) del presente apartado, incluidas las políticas a que se refiere el apartado 3.
- c) Un marco de gobernanza que aclare las funciones y responsabilidades de las partes interesadas pertinentes a nivel nacional, que sustente la cooperación y la coordinación a nivel nacional, dirigida por el Centro Nacional de Ciberseguridad, entre las autoridades de control, los CSIRT nacionales de referencia y los puntos de contacto sectoriales, así como la coordinación y la cooperación entre dichos organismos y las autoridades competentes con arreglo a actos jurídicos sectoriales de la Unión.
- d) Un procedimiento que permita la evaluación de los riesgos de ciberseguridad.
- e) Las medidas estratégicas necesarias para garantizar la preparación, la capacidad de respuesta y la recuperación frente a incidentes. A tal fin, deberán recogerse mecanismos de cooperación entre los sectores público y privado.
- f) El marco de actuación para la coordinación con las autoridades competentes designadas conforme a la ley xxxx, por la que se transpone la Directiva (UE) 2022/2557 a efectos del intercambio de información sobre los riesgos, las ciberamenazas e incidentes, así como sobre riesgos, amenazas e incidentes no relacionados con la ciberseguridad y el ejercicio de las funciones de supervisión.
- g) Un plan de medidas para mejorar la concienciación de los ciudadanos en materia de ciberseguridad.

3. Asimismo, en el marco de la Estrategia Nacional de Ciberseguridad, se adoptarán, en particular, políticas relativas a las cuestiones siguientes:

- a) La ciberseguridad en la cadena de suministro de productos y servicios de Tecnologías de la Información y la Comunicación (en adelante, TIC) utilizadas por las entidades para la prestación de sus servicios.
- b) La inclusión y especificación de los requisitos en materia de ciberseguridad que deben aplicarse a los productos y servicios de las TIC en la contratación pública, incluidos aquellos relativos a la certificación de ciberseguridad, al cifrado y al uso de productos de ciberseguridad de código abierto, sin perjuicio de su incorporación adicional a la normativa reguladora de la contratación pública.
- c) La gestión de las vulnerabilidades, que incluyan medidas para la promoción y divulgación coordinada, con arreglo a lo dispuesto en el artículo 11.1.
- d) La disponibilidad general, la integridad y la confidencialidad del núcleo público de la internet abierta, así como la ciberseguridad, cuando proceda, de los centros de datos y de los cables submarinos de comunicaciones.



- e) El desarrollo y la integración de las tecnologías avanzadas destinadas a aplicar medidas de gestión de riesgos de ciberseguridad de última generación.
 - f) La promoción y desarrollo de la educación y la formación en materia de ciberseguridad, capacidades de ciberseguridad, sensibilización e iniciativas de investigación y desarrollo, así como orientaciones sobre buenas prácticas y controles en materia de ciberhigiene, destinadas a los ciudadanos, las partes interesadas y las entidades, así como de apoyo a las instituciones académicas y de investigación para el desarrollo, la mejora y la implantación de herramientas de ciberseguridad e infraestructuras de red seguras.
 - g) Los procedimientos y las herramientas para compartir información que apoye el intercambio voluntario de información sobre ciberseguridad entre las entidades.
 - h) De refuerzo de la ciberresiliencia y la base de referencia en materia de ciberhigiene de las pequeñas y medianas empresas, especialmente de las excluidas del ámbito de aplicación de la esta ley, proporcionando orientaciones y apoyo de fácil acceso para sus necesidades específicas.
 - i) De promoción de la ciberprotección activa como parte de una estrategia de defensa amplia, establecida por la autoridad al más alto nivel.
4. El Consejo Nacional de Ciberseguridad verificará el grado de cumplimiento de la Estrategia Nacional de Ciberseguridad, así como de los instrumentos de desarrollo que se aprueben en función de los indicadores que establezca. A tal fin, remitirá, con carácter anual, un informe al Consejo de Seguridad Nacional, que recoja a demás las propuestas de mejora y la necesidad o no de aprobar una nueva estrategia.

5. El Centro Nacional de Ciberseguridad notificará la Estrategia Nacional de Ciberseguridad a la Comisión en el plazo de tres meses a partir de su adopción. Se podrá excluir de tal notificación información con incidencia en la seguridad nacional.

Artículo 6. El Centro Nacional de Ciberseguridad.

El Centro Nacional de Ciberseguridad es la autoridad nacional competente única en materia de gobernanza de la ciberseguridad, encargada de la dirección, impulso y la coordinación, en el ámbito de esta ley, de todas las actividades necesarias para garantizar un elevado nivel de ciberseguridad en España y contribuir a la ciberseguridad de la Unión Europea.

Ejercerá como Autoridad nacional de gestión de crisis y punto de contacto único, y asumirá la superior dirección y coordinación de las autoridades de control y puntos de contacto sectoriales en el desarrollo de sus funciones de ejecución y supervisión, así como de los CSIRT nacionales de referencia.



Además, en el marco de esta ley, llevará a cabo los siguientes cometidos:

- a) Actuar como órgano superior para la gobernanza y coordinación de las actividades en materia de ciberseguridad previstas en esta ley y en su normativa de desarrollo sin perjuicio de las competencias que los diferentes órganos y organismos tienen legalmente establecidas.
- b) Ejercer como autoridad nacional competente en el ámbito de la ciberseguridad, sin perjuicio de la existencia de autoridades de control y puntos de contacto sectoriales bajo su coordinación.
- c) Informar al público sobre incidentes que afecten a más de una autoridad de control, cuando la difusión de dicha información sea necesaria para evitar un incidente o gestionar uno que ya se haya producido.
- d) Establecer, en situaciones de justificada necesidad aprobada mediante resolución motivada, con el asesoramiento de las autoridades de control, las obligaciones específicas necesarias para garantizar la seguridad de las redes y sistemas de información.
- e) Promover y aprobar, en su caso, el uso de estándares, guías, especificaciones, instrucciones técnicas, así como cualquier otra disposición en materia de seguridad de las redes y sistemas de información.

Asumirá, además, cualesquiera otras funciones que se le encomienden en el ámbito de la ciberseguridad nacional, sin perjuicio de las competencias legalmente reservadas a otros organismos e instituciones.

Artículo 7. Autoridades de control, punto de contacto único y puntos de contacto sectoriales.

1. Son autoridades de control, encargadas de las funciones de supervisión y ejecución a que se refiere el Capítulo VI de esta ley, las siguientes:

- a) El Ministerio de Defensa, a través del Centro Criptológico Nacional, para las entidades esenciales e importantes que, no siendo entidades críticas, se encuentren comprendidas en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre del Régimen jurídico del Sector Público.
- b) El Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y de la Secretaría de Estado de Digitalización e Inteligencia Artificial, para las entidades esenciales e importantes de los sectores de Infraestructura digital y Proveedores de servicios digitales, así como de las entidades importantes del resto de sectores, que no se hayan designado como entidades críticas.



- c) El Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad de la Secretaría de Estado de Seguridad, para las entidades críticas y para las entidades esenciales de los sectores no incluidos en las letras a) o b), así como para todas las entidades esenciales e importantes del sector de seguridad privada.

Para el ejercicio de esas funciones de supervisión y ejecución tendrán encomendadas las siguientes competencias:

- a) Establecer canales de comunicación con las entidades esenciales e importantes, entre los que se incluyen la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes prevista en el artículo 19.
- b) Recibir y realizar el seguimiento de las notificaciones sobre incidentes que sean presentadas en el marco de esta ley a través de los CSIRT nacionales de referencia.
- c) Informar al público sobre determinados incidentes, cuando la difusión de dicha información sea necesaria para evitar un incidente o gestionar uno que ya se haya producido.
- d) Participar, de forma voluntaria, en las revisiones inter pares organizadas con arreglo al artículo 19 de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022.
- e) Proponer las medidas de gestión de riesgos de ciberseguridad de obligado cumplimiento para las entidades incluidas en el ámbito de aplicación de esta norma.
- f) Cualquier otra atribuida en esta ley o en su desarrollo reglamentario.

2. El Centro Nacional de Ciberseguridad se constituye como punto de contacto único para ejercer una función de enlace que garantice la cooperación transfronteriza con las autoridades pertinentes en otros Estados miembros y, cuando proceda, con la Comisión y la Agencia de la Unión Europea para la Ciberseguridad (ENISA), así como para garantizar la cooperación intersectorial con otras autoridades competentes nacionales.

A tal fin, tendrá las siguientes competencias:

- a) Transmitir, a los puntos de contacto únicos de otros Estados miembros de la Unión Europea afectados, la información sobre los incidentes de ciberseguridad que tengan impacto transfronterizo.
- b) Remitir a la ENISA la información del registro de proveedores de servicios e infraestructuras digitales recogidos en el artículo 26.1.



- c) Remitir a la Comisión y al Grupo de Cooperación la información de entidades esenciales e importantes recogida en el artículo 4.3.
- d) Remitir a los CSIRT nacionales de referencia la correspondiente información sobre los incidentes significativos que puedan tener efectos perturbadores en los servicios esenciales e importantes que reciba de las autoridades de control, CSIRT o autoridades competentes de los correspondientes Estados miembros, para que adopten las medidas oportunas en el ejercicio de sus funciones.
- e) Elaborar y remitir a la ENISA, trimestralmente, el informe sobre el tipo y número de incidentes que se hayan comunicado de acuerdo con esta ley, sus efectos en los servicios prestados o en otros servicios y su carácter nacional o transfronterizo dentro de la Unión Europea, para lo que podrá recabar la información necesaria de las autoridades de control.
- f) Cualquier otra atribuida en esta ley o en su desarrollo reglamentario.

3. Por cada uno de los sectores relacionados en los anexos I y II, se designará, al menos, un órgano ministerial u organismo o entidad de derecho público vinculado o dependiente de la Administración General del Estado que será, en el marco de sus competencias, el punto de contacto especializado con el Centro Nacional de Ciberseguridad y las autoridades de control. Estos puntos de contacto sectoriales desempeñarán las siguientes funciones:

- a) Impulsar las políticas de ciberseguridad y velar por la aplicación y cumplimiento de las obligaciones derivadas de esta ley.
- b) Instar a las organizaciones que constituyen su comunidad de entidades competenciales y supervisar su adecuado auto registro, como entidad esencial o importante.
- c) Colaborar con el Centro Nacional de Ciberseguridad y las autoridades de control en el desarrollo de las siguientes actividades:
 - i. La identificación de las entidades esenciales e importantes de su comunidad de referencia.
 - ii. La elaboración los perfiles específicos de cumplimiento de obligaciones del artículo 15.3.
 - iii. La supervisión del cumplimiento por parte de las entidades esenciales e importantes de las obligaciones que se determinan en la presente ley.
 - iv. El establecimiento de los canales de comunicación oportunos con las entidades esenciales e importantes que, en su caso, serán desarrollados reglamentariamente.
- d) Cualquier otra que se le asigne reglamentariamente.

4. Las comunidades autónomas colaborarán con el Centro Nacional de Ciberseguridad, o en su caso con las autoridades de control, en impulsar y velar por el cumplimiento de las políticas de ciberseguridad y las obligaciones derivadas de esta ley; particularmente en la identificación y notificación de las entidades del artículo 4.



Artículo 8. Marco nacional de gestión de crisis de ciberseguridad.

1. El Centro Nacional de Ciberseguridad, como autoridad nacional de gestión de crisis de ciberseguridad, será responsable de la coordinación para la gestión de incidentes y crisis de ciberseguridad a gran escala.
2. Reglamentariamente, se establecerán las capacidades, los activos y los procedimientos que habrán de desplegarse en caso de que se produzca una crisis de ciberseguridad.
3. Asimismo, el Centro Nacional de Ciberseguridad adoptará un plan de respuesta a incidentes y crisis de ciberseguridad a gran escala en el que se fijen los objetivos y las medidas de la gestión de los incidentes y las crisis de ciberseguridad a gran escala. Dicho plan deberá incluir, en todo caso:
 - a) Los objetivos de las medidas y actividades en materia de preparación.
 - b) Las funciones y responsabilidades asignadas a las autoridades con competencia en materia de ciberseguridad.
 - c) los procedimientos de gestión de crisis de ciberseguridad, incluida su integración en el marco general de gestión de crisis, y los canales para el intercambio de información.
 - d) Las medidas de preparación, que deberán incluir los ejercicios y las actividades de formación.
 - e) Las partes interesadas públicas y privadas pertinentes y la infraestructura implicada.
 - f) Los procedimientos y mecanismos para garantizar la participación y apoyo de España en la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel de la Unión Europea.

Artículo 9. Equipos de respuesta a incidentes de ciberseguridad (CSIRT) nacionales de referencia.

1. Son equipos de respuesta a incidentes de ciberseguridad (CSIRT) nacionales de referencia, en materia de seguridad de las redes y sistemas de información, los siguientes:
 - 1º El CCN-CERT, del Centro Criptológico Nacional (CCN), al que corresponde la comunidad de referencia constituida por las entidades consideradas esenciales o importantes de acuerdo con esta Ley que se encuentren incluidas dentro del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.En todo caso, el CCN-CERT, siguiendo las instrucciones del Centro Nacional de Ciberseguridad, ejercerá la coordinación nacional de la respuesta técnica de los CSIRT en incidentes significativos o supuestos de especial gravedad.



2º El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, al que corresponde la comunidad de referencia constituida por las entidades consideradas esenciales o importantes de acuerdo con esta Ley y que no se encuentren incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

3º El ESPDEF-CERT, del Mando Conjunto del Ciberespacio, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran y, necesariamente, en las relativas a incidentes de entidades con incidencia en la Defensa Nacional, en cuyo caso se coordinarán con él aquellos aspectos que pueda afectar a la Defensa Nacional, al Ministerio de Defensa o a la Operatividad de las Fuerzas Armadas; sin perjuicio de lo dispuesto en este artículo para los incidentes que afecten a entidades críticas.

2. En los incidentes que afecten a entidades catalogadas como críticas de acuerdo con la ley xxxx, el CSIRT-MIR-PJ de la Oficina de Coordinación de Ciberseguridad (OCC) operará conjuntamente con el CSIRT de referencia correspondiente.
3. El Centro Nacional de Ciberseguridad asumirá las funciones de coordinación de los CSIRT nacionales de referencia en el ámbito de esta ley, en concreto:
 - a) Garantizará la coordinación de los CSIRT nacionales e internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.
 - b) Cooperará e intercambiará información pertinente con comunidades sectoriales o intersectoriales de entidades esenciales e importantes y, cuando proceda, con sus proveedores o prestadores de servicios, conforme a lo establecido en el artículo 30.
 - c) Coordinará la cooperación efectiva, eficiente y segura de sus CSIRT en la red de CSIRT de la Unión Europea.
 - d) Ejercerá la superior coordinación de las relaciones de cooperación que los CSIRT nacionales de referencia podrán establecer con equipos nacionales de respuesta a incidentes de seguridad informática de terceros países de acuerdo con el apartado 5 de este artículo.
 - e) Coordinará y canalizará la participación de los CSIRT nacionales de referencia en las revisiones inter pares organizadas con arreglo a lo dispuesto en el artículo 13 de esta ley.



4. Sin perjuicio de lo dispuesto para los ciberincidentes que afecten a entidades críticas, cuando las actividades que desarrollen puedan afectar a una entidad del sector de la seguridad privada, o en lo concerniente a la averiguación de delitos o descubrimiento y aseguramiento de delincuentes por parte de las Fuerzas y Cuerpos de Seguridad, los CSIRT nacionales de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad, de la Secretaría de Estado de Seguridad, asegurando su acceso a toda la información necesaria para el desempeño de sus funciones.
El Centro Nacional de Ciberseguridad garantizará la coordinación mencionada en el párrafo anterior.
5. Cuando una entidad con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, este pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas. En el caso de que así fuera, lo pondrá de inmediato en conocimiento de su CSIRT nacional de referencia, quien informará al ESPDEF-CERT del Mando Conjunto del Ciberespacio a través de los canales establecidos. Así mismo, los CSIRT nacionales de referencia afectados informarán al ESPDEF-CERT de todos los incidentes que les hayan sido notificados por los operadores con incidencia en la Defensa Nacional de su comunidad de referencia, así como de la evolución de la gestión del incidente. En estos casos, cuando la operatividad de las Fuerzas Armadas lo requiera, el ESPDEF-CERT podrá apoyar directamente a la entidad afectada en coordinación con el CSIRT nacional de referencia.
6. Los CSIRT nacionales de referencia podrán establecer relaciones de cooperación con equipos nacionales de respuesta a incidentes de seguridad informática de terceros países, posibilitando un intercambio de información eficaz, eficiente y seguro, utilizando los protocolos de intercambio de información pertinentes, incluido el protocolo TLP y datos personales, de conformidad con la legislación de la Unión en materia de protección de datos.
7. Los CSIRT nacionales de referencia podrán cooperar con equipos nacionales de respuesta a incidentes de seguridad informática de terceros países u organismos equivalentes de terceros países, en particular con el fin de proporcionarles asistencia en materia de ciberseguridad.
8. Cada CSIRT nacional de referencia dispondrá de los recursos adecuados para llevar a cabo eficazmente sus cometidos.
9. Los CSIRT nacionales de referencia tendrán a su disposición una infraestructura de comunicación e información apropiada, segura y resiliente para el intercambio de información con las entidades esenciales e importantes y otras partes interesadas pertinentes. Para ello, cada CSIRT nacional de referencia contribuirá al despliegue de herramientas seguras para el intercambio de información.



Artículo 10. Obligaciones, capacidades técnicas y competencias de los CSIRT nacionales de referencia.

1. Los CSIRT nacionales de referencia deberán cumplir los siguientes requisitos:
 - a) Garantizar que sus canales de comunicación estén disponibles, evitando los fallos puntuales simples, y deben contar, en todo momento, con varios medios de comunicación para ser contactados y contactar con otros. Asimismo, deben especificar cuáles son sus los canales de comunicación y comunicárselos a los grupos de usuarios y los socios colaboradores.
 - b) Sus dependencias y las de los sistemas de información de apoyo deben estar situadas en lugares que reúnan las necesarias condiciones de seguridad conforme a la legislación aplicable en cada caso.
 - c) Estar dotados de un sistema adecuado para gestionar y canalizar las solicitudes, que facilite, en particular, la efectividad y eficiencia de los traspasos.
 - d) Garantizar la confidencialidad y fiabilidad de sus operaciones.
 - e) Contar con personal suficiente para garantizar la disponibilidad de sus servicios en todo momento y velar por la adecuada formación de su personal.
 - f) Estar dotados de sistemas redundantes y espacios de trabajo de reserva para garantizar la continuidad de sus servicios.
2. Los CSIRT nacionales de referencia tendrán, en sus respectivos ámbitos de actuación, las siguientes atribuciones:
 - a) Realizar un seguimiento y análisis de las ciberamenazas, las vulnerabilidades y los incidentes producidos a escala nacional y, previa solicitud, prestar asistencia a las entidades esenciales e importantes afectadas en la supervisión en tiempo real o inmediato de sus redes y sistemas de información, en coordinación con las autoridades de control.
 - b) Difundir alertas tempranas, alertas, avisos e información sobre las ciberamenazas, las vulnerabilidades y los incidentes producidos entre las entidades esenciales e importantes afectadas, así como entre las autoridades de control y otras partes interesadas en tiempo real o inmediato
 - c) Responder a incidentes y prestar asistencia a las entidades esenciales e importantes en atención al grado de afectación a los servicios o los datos almacenados, transmitidos o tratados.



- d) Recopilar y analizar datos forenses y efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación en materia de ciberseguridad.
- e) Proporcionar, a petición de una entidad esencial o importante afectada, una exploración proactiva de las redes y sistemas de información de la entidad afectada para detectar vulnerabilidades que puedan tener una repercusión significativa.
- f) Participar en la red de CSIRT de la Unión Europea prevista en el artículo 15 de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, y en la Red Europea de Centros de Operaciones de Ciberseguridad para potenciar el intercambio automático de indicadores de compromiso que facilite en tiempo real información sobre ciberataques en curso, y prestar asistencia mutua, de conformidad con sus capacidades y competencias, a otros miembros de la red de CSIRT cuando la soliciten.
- g) Contribuir al despliegue de herramientas seguras de intercambio de información.
- h) Cuando proceda, actuar como coordinador a efectos del proceso de divulgación coordinada de vulnerabilidades.

En la ejecución de estas actuaciones se podrá dar prioridad a cometidos determinados sobre la base de un enfoque basado en el riesgo.

3. Los CSIRT nacionales de referencia podrán llevar a cabo una exploración proactiva no intrusiva de las redes y sistemas de información de acceso público de sus respectivas comunidades de referencia. Dicha exploración se llevará a cabo con la finalidad de detectar vulnerabilidades y configuraciones inseguras en las redes y sistemas de información e informar a las entidades afectadas. Dicha exploración no deberá tener ningún impacto negativo en el funcionamiento de los servicios de las entidades, ni podrá afectar a la intimidad de las personas.

4. Los CSIRT nacionales de referencia, bajo la coordinación del Centro Nacional de Ciberseguridad, cooperarán con las partes interesadas del sector privado, y fomentarán la adopción y utilización de prácticas comunes o normalizadas, sistemas de clasificación y taxonomías en relación con:

- a) Los procedimientos de gestión de incidentes.
- b) La gestión de crisis de ciberseguridad, y
- c) La divulgación coordinada de las vulnerabilidades.

Artículo 11. *Divulgación coordinada de las vulnerabilidades.*



1. El Centro Nacional de Ciberseguridad designará al CSIRT nacional de referencia que realizará las funciones de organismo coordinador a efectos de la divulgación coordinada de las vulnerabilidades, ejerciendo de intermediario de confianza y facilitando, cuando sea necesario, la interacción entre la persona física o jurídica que notifique una vulnerabilidad y el fabricante o proveedor de los productos de TIC o los servicios de TIC potencialmente vulnerables, a petición de cualquiera de las partes. Los cometidos del CSIRT nacional de referencia coordinador incluirán:

- a) Identificar y contactar a las entidades afectadas.
- b) Prestar asistencia a las personas físicas o jurídicas que notifican una vulnerabilidad.
- c) Negociar los plazos de divulgación y gestionar las vulnerabilidades que afectan a múltiples entidades.

2. En el desempeño de su función de coordinación, el CSIRT nacional de referencia designado garantizará que las personas físicas o jurídicas que así lo soliciten puedan comunicar de forma anónima una vulnerabilidad detectada. De la misma forma garantizará que se lleve a cabo un seguimiento diligente de la vulnerabilidad notificada. Cuando la vulnerabilidad notificada pueda repercutir significativamente en entidades de más de un Estado miembro, cooperará, cuando proceda, con los CSIRT designados como coordinadores en el marco de la red europea de CSIRT.

Artículo 12. *Cooperación nacional.*

El Centro Nacional de Ciberseguridad ejercerá los siguientes cometidos en materia de cooperación nacional:

- a) Con objeto de garantizar el cumplimiento efectivo de sus funciones y obligaciones, el Centro Nacional de Ciberseguridad cooperará y colaborará con los órganos y organismos públicos con competencias en materia de Seguridad Nacional, Defensa Nacional, seguridad pública, seguridad ciudadana, administración digital, protección de datos de carácter personal, así como con cualquier entidad con competencias dentro de su ámbito de aplicación, particularmente con las autoridades nacionales en el ámbito de aviación civil y seguridad aérea, con los organismos de supervisión relativos a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, con las autoridades competentes en materia de resiliencia operativa digital del sector financiero, con las autoridades nacionales de reglamentación en el marco del Código Europeo de las Comunicaciones Electrónicas, y con las autoridades competentes en materia de resiliencia de las entidades críticas.
- b) Cooperará e intercambiará periódicamente información con las autoridades competentes designadas conforme a la ley XXXX sobre la identificación de entidades críticas, los riesgos, las ciberamenazas y los incidentes relacionados con las TIC, así como sobre los riesgos, las amenazas y los incidentes no cibernéticos que afecten a



entidades esenciales identificadas como entidades críticas, y sobre las medidas adoptadas en respuesta a los mismos. También intercambiará información en relación con los incidentes relacionados con las TIC y ciberamenazas con las autoridades competentes en materia de identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, resiliencia operativa digital del sector financiero, y comunicaciones electrónicas.

- c) Cooperar con las autoridades competentes en los sectores sometidos a la normativa específica en materia de ciberseguridad con la finalidad de armonizar la normativa.
- d) Cooperará con las autoridades competentes de otros Estados miembros de la Unión Europea para identificar las entidades esenciales e importantes que ofrezcan sus servicios en varios Estados miembros, así como para identificar y resolver los incidentes que puedan producirse en el marco de esta ley y que afecten a varios Estados miembros.

Artículo 13. *Cooperación en el ámbito de la Unión Europea.*

El Centro Nacional de Ciberseguridad ejercerá los siguientes cometidos en materia de cooperación en el ámbito de la Unión Europea:

- a) Asumir la representación nacional en el Grupo de Cooperación previsto en el artículo 14 de la Directiva 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, establecido a fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados Miembros y para fortalecer la confianza y la colaboración, así como coordinar la participación de las autoridades de control y CSIRT nacionales de referencia en sus grupos trabajo.
- b) Asumir la representación nacional en la Red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe), prevista en el artículo 16 de la Directiva 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, creada con el fin de respaldar la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio regular de información relevante entre los Estados miembros y la Unión Europea.
- c) Garantizar la cooperación efectiva de los CSIRT nacionales en la Red de CSIRT de la Unión Europea, prevista en el artículo 15 de la Directiva 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, así como con la red europea de Centros de Operaciones de Ciberseguridad con vistas a contribuir al refuerzo de la confianza, la seguridad y la promoción de una cooperación operativa rápida y eficaz entre los Estados miembros.



d) Coordinar la participación en las revisiones inter pares conforme a lo establecido en el artículo 19 de la Directiva 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022.

e) Asumir la representación nacional en el Consejo de Administración de la ENISA y en la red de funcionarios de enlace nacionales.

Capítulo III

Medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación

Artículo 14. *Gobernanza.*

1. Los órganos de dirección de las entidades esenciales e importantes serán responsables de aplicar las medidas para la gestión de riesgos de ciberseguridad incluidas en esta ley, de supervisar su implantación efectiva y, en su caso, asumirán la responsabilidad por su incumplimiento.

Todo ello sin perjuicio de las normas aplicables en materia de responsabilidad de la administración pública, empleadas y empleados públicos, y los cargos electos o designados.

2. Igualmente, los miembros de los órganos de dirección de las entidades esenciales e importantes deberán recibir formación adecuada de forma periódica al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad. Así mismo, los órganos de dirección deberán organizar periódicamente formaciones similares para sus empleados.

Artículo 15. *Medidas generales para la gestión de riesgos de ciberseguridad.*

1. El Centro Nacional de Ciberseguridad determinará las medidas técnicas, operativas y de organización adecuadas y proporcionadas que las entidades esenciales e importantes deberán implantar para gestionar los riesgos que se evidencien en el análisis previo para la seguridad de las redes y sistemas de información que utilizan en sus operaciones o en la prestación de sus servicios y para prevenir o minimizar la repercusión de los incidentes en los destinatarios de sus servicios y en otros servicios, y velará para que las autoridades de control insten a las entidades esenciales e importantes para que adopten tales medidas.

2. Las medidas de seguridad a las que se refiere el apartado anterior tomarán como base las contempladas tanto en el Esquema Nacional de Seguridad como en normas técnicas europeas e internacionales equivalentes; garantizarán un nivel adecuado de seguridad de las redes y sistemas de información, así como de su entorno físico, adecuado en relación con los riesgos planteados; e incluirán, al menos, los siguientes elementos:



- a) Las políticas de seguridad de las redes y sistemas de información y el análisis de riesgos;
- b) La gestión de incidentes;
- c) La continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis;
- d) La seguridad de la cadena de suministro, que deberá incluir los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos, así como el punto de contacto de seguridad principal para cada uno de los proveedores;
- e) La seguridad en la adquisición, el desarrollo y el mantenimiento de redes y sistemas de información, incluida la gestión y divulgación de las vulnerabilidades;
- f) Las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad;
- g) Las prácticas básicas de ciberhigiene y de formación en ciberseguridad;
- h) Las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado;
- i) La seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos;
- j) El uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.

En el caso de las entidades obligadas por el Real Decreto 311/2022, de 3 de mayo, el correspondiente Perfil de Cumplimiento Específico del Esquema Nacional de Seguridad para las entidades esenciales e importantes acreditará el cumplimiento de las medidas de gestión de riesgos de ciberseguridad de esta norma. Lo mismo resultará de aplicación a aquellas entidades esenciales o importantes que no estando sujetas al Real Decreto 311/2022 obtengan voluntariamente una evaluación satisfactoria contra el Perfil de Cumplimiento Específico del Esquema Nacional de Seguridad.

Las autoridades de control proporcionarán al Centro Nacional de Ciberseguridad toda la información necesaria para la determinación de estas medidas.

3. A fin de tener debidamente en cuenta los diferentes grados de exposición de las entidades a los riesgos, el tamaño de la entidad y la probabilidad de que se produzcan incidentes y su gravedad, incluidas sus repercusiones sociales y económicas, así como la especificidad de determinados sectores y operadores, el Centro Nacional de Ciberseguridad podrá aprobar perfiles específicos de cumplimiento de obligaciones.

Estos perfiles de cumplimiento tendrán en cuenta las vulnerabilidades específicas de cada proveedor directo, así como la calidad general de los productos y las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro, tomando en consideración los resultados de las



evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas realizadas de conformidad con el artículo 22, apartado 1 de la Directiva (UE) 2022/2555.

Además, los perfiles específicos de cumplimiento se diseñarán de manera incremental sobre las medidas de gestión de riesgos de ciberseguridad generales de los apartados 1 y 2.

Los puntos de contacto sectoriales colaborarán con las autoridades de control en la elaboración de estos perfiles específicos de cumplimiento para su aprobación por el Centro Nacional de Ciberseguridad, que garantizará su armonización y coherencia.

4. Las entidades esenciales e importantes deberán demostrar el cumplimiento de las obligaciones a las que se refiere este artículo. En el caso de las entidades esenciales, el cumplimiento se evidenciará mediante la obtención y mantenimiento de una certificación de conformidad acreditativa. Las entidades importantes podrán optar entre la antedicha certificación o realizar una autoevaluación de la postura de seguridad.

Las entidades esenciales o importantes que se encuentren expresamente comprendidas en el ámbito de aplicación del Real Decreto 311/2022, de 3 de mayo, observarán lo dispuesto por este en materia de Certificación de la Conformidad con el Esquema Nacional de Seguridad.

El Centro Nacional de Ciberseguridad establecerá los procedimientos de certificación de acuerdo con los principios de necesidad, proporcionalidad y eficiencia. Además, procurará que el procedimiento y los requisitos para la adquisición de esta certificación se diseñen de manera que esta acredite al mismo tiempo el cumplimiento del esquema nacional de seguridad y las normas técnicas internacionales en sus niveles concordantes

5. Estas medidas se aplicarán a los activos o sistemas que se utilicen para la prestación de sus servicios u operaciones y deberán figurar en un documento suscrito por el responsable de seguridad de la información denominado declaración de aplicabilidad de sistemas. Dicho documento deberá remitirse a la autoridad de control correspondiente dentro de los seis meses siguientes a la adquisición de la condición de entidad esencial o importante.

6. Las entidades esenciales e importantes deberán aplicar adecuadamente los actos de ejecución adoptados por la Comisión Europea por los que se establezcan los requisitos técnicos y metodológicos de las medidas recogidas en el apartado 2 con respecto a las entidades recogidas en el artículo 26.1.

Asimismo, el Centro Nacional de Ciberseguridad o, en su caso las autoridades de control instarán a las entidades esenciales e importantes distintas de las señaladas en el párrafo anterior a que apliquen los actos de ejecución adoptados por la Comisión Europea.

Artículo 16. *Responsable de la seguridad de la información.*



1. Las entidades esenciales e importantes designarán a una persona, unidad u órgano colegiado como responsable de la seguridad de la información, que ejercerá las funciones de punto de contacto y coordinación técnica con las autoridades de control y con los CSIRT nacionales de referencia. En el supuesto de que el responsable de la seguridad de la información sea una unidad u órgano colegiado, se deberá designar a una persona física como representante, así como un sustituto de este que asumirá sus funciones en casos de ausencia, vacante o enfermedad.

2. Las entidades esenciales o importantes comunicarán a las autoridades de control la designación del responsable de la seguridad de la información dentro del plazo de tres meses desde su designación. Asimismo, comunicarán los sucesivos nombramientos y ceses en el plazo de un mes desde que aquellos se produzcan.

3. En las entidades esenciales, el responsable de la seguridad de la información, su persona física representante en caso de ser un órgano colegiado y su sustituto; independientemente de los requisitos de capacidad técnica y formación, deberán ser personal acreditado por el Ministerio del Interior. En el caso de tratarse de entidades esenciales que también tengan la consideración de críticas conforme a la ley XXXXXXXX, esta obligación será asimismo extensiva al resto de personal encargado de realizar las labores de ciberseguridad previstas en esta Ley.

La forma de obtención, mantenimiento y pérdida de la condición de personal acreditado al que se refiere el párrafo anterior se regulará reglamentariamente de acuerdo con lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y dentro del marco competencial establecido en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. La determinación de sus funciones, así como, en su caso, de la formación específica necesaria, será responsabilidad del Centro Nacional de Ciberseguridad.

El responsable de la seguridad de la información tendrá las siguientes funciones:

- a) Elaborar y someter a la aprobación de la organización la estrategia y políticas de seguridad, que deberán incluir las medidas de gestión de riesgos de ciberseguridad, técnicas y organizativas y proporcionadas establecidas en esta norma.
- b) Supervisar y desarrollar la aplicación de las políticas de seguridad, y procedimientos derivados de la organización, su efectividad y llevar a cabo controles periódicos de seguridad.
- c) Supervisar el cumplimiento de la normativa aplicable en materia de seguridad de las redes y sistemas de información.



- d) Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, en lo relativo a aspectos tanto físicos como lógicos.
- e) Gestionar los incidentes de ciberseguridad recogidos en el artículo 17.
- f) Remitir a las autoridades de control, a través de los CSIRT nacionales de referencia, sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios y de las vulnerabilidades detectadas.
- g) Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad de control, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- h) Recopilar, preparar y suministrar información o documentación a la autoridad de control y a los CSIRT nacionales nacional de referencia, previa solicitud o por propia iniciativa.
- i) Elaborar y suscribir el documento de aplicabilidad de sistemas o activos.
- j) Velar por el cumplimiento de empresas externas y proveedores de los criterios de seguridad de la información establecidos por la entidad.

Para desarrollar estas funciones, podrá contar con la colaboración de servicios prestados por terceros.

4. Las entidades esenciales garantizarán que el responsable de la seguridad de la información cumpla los siguientes requisitos:

- a) Contar con personal con conocimientos especializados y experiencia en materia de ciberseguridad, desde los puntos de vista jurídico, organizativo y técnico, adecuados al desempeño de sus funciones.
- b) Contar con los recursos necesarios para el desarrollo de sus funciones.
- c) Ostentar una posición en la organización que facilite el desarrollo de sus funciones, participando de forma adecuada y en todas las cuestiones relativas a la seguridad, y manteniendo una comunicación real y efectiva con el consejo de administración.
- d) Mantener la debida independencia respecto de los responsables de las redes y los sistemas de información.

Artículo 17. *Gestión de incidentes de seguridad.*



1. Las entidades esenciales e importantes deberán gestionar y resolver los incidentes de seguridad que afecten a las redes y sistemas de información propios. En el caso de que estos incidentes afecten a redes y sistemas ajenos, deberán adoptar las medidas necesarias para garantizar que dichas acciones se lleven a cabo por los proveedores externos.

Esta obligación se refiere tanto a los incidentes que detecte la propia entidad o proveedor como a aquellos que comunique la autoridad de control, a través de los CSIRT nacionales de referencia, cuando tenga conocimiento de alguna circunstancia que haga sospechar de la existencia de un incidente.

2. Sin perjuicio de lo previsto en el apartado primero, las entidades esenciales e importantes podrán solicitar voluntariamente la ayuda especializada de su CSIRT nacional de referencia para la gestión de los incidentes, debiendo en tales casos atender a las indicaciones que reciban de este para resolver el incidente, mitigar sus efectos y reponer los sistemas afectados.

3. Para la resolución de los incidentes, las entidades esenciales e importantes deberán aplicar los aspectos pertinentes de la política de gestión de la seguridad de las redes y sistemas de información, así como las obligaciones específicas que en su caso establezcan las autoridades de control.

Artículo 18. *Obligaciones de notificación.*

1. Las entidades esenciales e importantes deberán notificar a la autoridad de control sin demora indebida, a través de su CSIRT nacional de referencia, cualquier incidente significativo que se haya producido en su operativa o en la prestación de sus servicios, según se determine reglamentariamente, en base a su peligrosidad e impacto. Cuando proceda, notificarán igualmente a los destinatarios de sus servicios que pudieran resultar afectados, en el menor plazo posible, los incidentes significativos susceptibles de causarles perjuicios de relevancia. Estas notificaciones se realizarán a través del responsable de la seguridad de la información.

Las autoridades de control garantizarán que las entidades obligadas notifiquen, entre otros detalles, cualquier información que permita determinar las repercusiones transfronterizas del incidente.

2. Las notificaciones que realicen las entidades esenciales o importantes se referirán a los incidentes que afecten a las redes y sistemas de información empleados en su operativa o en la prestación de sus servicios, tanto si son redes y servicios propios, como si pertenecen a proveedores externos.

3. Los CSIRT nacionales de referencia utilizarán la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes para facilitar y automatizar los procesos de notificación, las comunicaciones e informaciones sobre incidentes y dispondrán de acceso, confidencial



y completo, a la información íntegra, siempre que sea relativa a sus respectivas responsabilidades y competencias.

4. La obligación de notificación de incidentes, no obsta al cumplimiento del deber legal de denunciar aquellos hechos que revistan caracteres de delito ante las autoridades competentes, de acuerdo con lo dispuesto en los artículos 259 y siguientes de la Ley de Enjuiciamiento Criminal, ni a la competencia para su investigación. Independientemente de las obligaciones establecidas en este artículo, en caso de que se produzcan incidentes que tengan características delictivas, se actuará conforme a lo establecido en el artículo 21.

5. Las entidades esenciales e importantes comunicarán a las personas físicas y jurídicas destinatarias de sus servicios, a la mayor brevedad, cualquier ciberamenaza significativa que les pueda afectar, así como las medidas o soluciones que pueden aplicar como respuesta. Asimismo, actuarán de la misma manera con las ciberamenazas y ciberincidentes que les notifique la autoridad de control o su CSIRT nacional de referencia.

6. Las entidades afectadas presentarán, a la mayor brevedad posible, a la autoridad de control, a través de su CSIRT nacional de referencia, lo siguiente:

- a) Sin demora indebida y, en cualquier caso, en el plazo de veinticuatro horas desde que se haya tenido constancia de que se ha producido un incidente significativo, una alerta temprana en la que se indicará, cuando proceda, si cabe sospechar que el incidente significativo responde a una acción ilícita o malintencionada o puede tener repercusiones transfronterizas.
- b) En el plazo máximo de setenta y dos horas desde que se haya tenido constancia de que se ha producido el incidente significativo, una notificación del incidente en la que se actualizará, cuando proceda, la información contemplada en la letra a) y se expondrá una evaluación inicial del incidente significativo, incluyendo su peligrosidad e impacto, así como los indicadores de compromiso, cuando estén disponibles.

Para los prestadores de servicios de confianza, cuando el incidente afecte a la prestación de sus servicios, el plazo del párrafo anterior se reducirá a un máximo de veinticuatro horas.

Los informes referidos en este artículo serán remitidos a la autoridad de control de manera inmediata.

- c) A instancias de su CSIRT nacional de referencia o, en su caso, de la autoridad de control, un informe intermedio con las actualizaciones que se hayan producido sobre la situación.



- d) Un informe final, a más tardar un mes después de presentar la notificación del incidente contemplada en la letra b), en el que se recojan los siguientes elementos:
- i. Una descripción detallada del incidente, incluyendo su peligrosidad e impacto.
 - ii. El tipo de amenaza o causa principal que probablemente haya desencadenado el incidente.
 - iii. Las medidas paliativas que se hayan aplicado o se estén aplicando.
 - iv. Cuando proceda, las repercusiones transfronterizas del incidente.
 - v. Indicadores de compromiso (IoCs), así como Tácticas, Técnicas y Procedimientos (TTPs) detectados en el incidente.
- e) En caso de que el incidente siga en curso en el momento de la presentación del informe final contemplado, las entidades afectadas presentarán un informe de situación en ese momento y un informe final en el plazo de un mes a partir de que hayan gestionado el incidente.

8. La autoridad de control o el CSIRT nacional de referencia en cada caso ofrecerá, sin demora indebida y, cuando sea posible, en el plazo de veinticuatro horas tras la recepción de la alerta temprana a que se refiere el apartado 6, letra a), una respuesta a la entidad notificante, en particular sus comentarios iniciales sobre el incidente significativo y, a instancias de la entidad, una orientación o asesoramiento operativo sobre la aplicación de posibles medidas paliativas.

Cuando el CSIRT nacional de referencia no sea el destinatario inicial de la notificación a que se refiere el apartado 1, la orientación será proporcionada por la autoridad de control en colaboración con el CSIRT nacional de referencia. El CSIRT nacional de referencia prestará apoyo técnico adicional cuando así lo solicite la entidad afectada. Cuando se sospeche que el incidente es de naturaleza delictiva, el CSIRT nacional de referencia o la autoridad de control también proporcionará orientación a efectos de denunciar el incidente significativo ante las autoridades encargadas de hacer cumplir la ley.

9. Cuando proceda, y en particular si el incidente significativo afecta a dos o más Estados miembros, el Centro Nacional de Ciberseguridad informará, sin demora indebida, a los demás Estados miembros afectados y a la ENISA. Dicha información incluirá el tipo de información recibida de conformidad con el apartado 6. Al hacerlo, preservará, de conformidad con el ordenamiento jurídico de la Unión o nacional, la seguridad y los intereses comerciales de la entidad, así como la confidencialidad de la información facilitada.

10. Cuando sea necesario el conocimiento general del incidente significativo, para evitar otros incidentes significativos o hacer frente a otro incidente significativo en curso, o cuando la divulgación redunde en el interés público, el Centro Nacional de Ciberseguridad, las autoridades de control y los CSIRT o las autoridades competentes de otros Estados



miembros afectados, podrán informar públicamente, previa consulta con la entidad afectada, del incidente significativo o exigir a la entidad que lo haga.

11. El Centro Nacional de Ciberseguridad deberá remitir sin demora las notificaciones recibidas de las autoridades de control en virtud de lo previsto en el apartado 1 a los puntos de contacto únicos de los Estados miembros afectados.

12. El Centro Nacional de Ciberseguridad presentará cada tres meses a la ENISA un informe de síntesis que incluya datos anonimizados y agregados sobre los incidentes significativos y los incidentes, las ciberamenazas y los cuasiincidentes notificados de conformidad con el apartado 1 y con el artículo 29.

13. Los CSIRT nacionales de referencia, a través de la Oficina de Coordinación de Ciberseguridad, dependiente de la Secretaría de Estado de Seguridad, facilitarán a las autoridades competentes en materia de resiliencia de las entidades críticas designadas conforme a lo establecido en la ley XXXX, la información sobre los incidentes significativos, los incidentes, las ciberamenazas y los cuasiincidentes notificados de conformidad con el apartado 1 y las notificaciones voluntarias realizadas conforme al artículo 29 por parte de las entidades equivalentes a entidades críticas.

14. Las notificaciones recogidas en este artículo deberán sujetarse a lo dispuesto en la Instrucción Nacional de Notificación y Gestión de Ciberincidentes.

Artículo 19. Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

1. Las obligaciones de notificación deberán realizarse preferentemente a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes. Esta plataforma será adaptada, mantenida y gestionada por el CCN-CERT bajo la dirección del Centro Nacional de Ciberseguridad sin perjuicio de los mecanismos de colaboración necesarios con el INCIBE-CERT y el ESPDEF-CERT. Los requisitos, procedimientos, mecanismos y responsabilidades de la operación de la plataforma por parte de los usuarios se desarrollarán reglamentariamente. La citada plataforma podrá usarse para las notificaciones exigidas por las regulaciones sectoriales.

2. Asimismo, esta plataforma permitirá que las entidades esenciales e importantes, el Centro Nacional de Ciberseguridad, las autoridades de control y los CSIRT nacionales de referencia, intercambien información técnica y puedan realizar el seguimiento de los incidentes de manera segura y confiable, sin perjuicio de los requisitos específicos que apliquen en materia de protección de datos de carácter personal.

3. El diseño y la gestión de la plataforma garantizarán la disponibilidad, autenticidad, integridad, trazabilidad y confidencialidad de la información, así como la transparencia del tratamiento de los datos ante el Centro Nacional de Ciberseguridad, las autoridades de control y los CSIRT nacionales de referencia.



4. La plataforma dispondrá, asimismo, de diversos canales de comunicación entre el Centro Nacional de Ciberseguridad, las autoridades de control, puntos de contacto sectoriales y los CSIRT nacionales de referencia, y garantizará su acceso a toda la información relativa a los incidentes, dentro del ámbito de su competencia. En concreto, podrán acceder a toda aquella información que les permita realizar en todo momento el seguimiento y control de su estado de situación y gestión técnica. Igualmente, tendrán acceso a todos los datos estadísticos alojados en la plataforma al objeto de conocer el estado de situación dentro del ámbito de la ciberseguridad nacional.

5. Asimismo, deberá realizarse a través de la plataforma el procedimiento de notificación y gestión de incidentes, que estará disponible ininterrumpidamente 24 horas al día, todos los días del año, y dispondrá como mínimo de las siguientes capacidades:

- a) Capacidad de gestión de ciberincidentes, con incorporación de taxonomía, criticidad y notificaciones a terceros.
- b) Capacidad de intercambio de información sobre ciberamenazas.
- c) Capacidad de análisis de muestras.
- d) Capacidad de registro y notificación de vulnerabilidades.
- e) Capacidad de comunicaciones seguras entre los actores involucrados en diferentes formatos y plataformas.
- f) Capacidad de intercambio masivo de datos.
- g) Generación de estadísticas e informes agregados.

6. Los gestores y usuarios de la plataforma, de acuerdo con sus respectivas competencias, desarrollarán los correspondientes tratamientos de protección de datos personales.

Artículo 20. *Información sobre incidentes.*

1. Los CSIRT nacionales de referencia proporcionarán a las entidades esenciales e importantes notificantes información sobre el seguimiento de la notificación de un incidente, y, en particular, aquella que pueda facilitar una gestión eficaz del mismo.

Adicionalmente, las autoridades de control y los CSIRT nacionales de referencia, proporcionarán a las entidades esenciales e importantes que pudieran verse afectados por dichos incidentes, la información que pudiera serles relevante para prevenir y en su caso resolver el incidente.

2. Al proporcionar la información a la que se refiere el apartado anterior, se velará por los intereses comerciales de las entidades esenciales e importantes, tomando en consideración la confidencialidad de la información.

Artículo 21. *Actuaciones ante incidentes con carácter presuntamente delictivo.*



1. Se considerarán ciberincidentes con carácter presuntamente delictivo todos aquellos que tengan la consideración de incidentes significativos en los que pueda existir intencionalidad y no se traten de hechos accidentales o fortuitos.
2. Para determinar el posible carácter delictivo de los incidentes que sean notificados a las autoridades de control, a través de los CSIRT nacionales de referencia, estas deberán trasladar a la Oficina de Coordinación de Ciberseguridad la información que posean sobre estos incidentes. La Oficina de Coordinación de Ciberseguridad podrá requerir a las entidades afectadas, a las autoridades de control y a los CSIRT nacionales de referencia, la información adicional relacionada con el incidente que se estime necesaria a tales efectos.
3. La Oficina de Coordinación de Ciberseguridad, en cumplimiento de lo dispuesto en el artículo 262 de la Ley de Enjuiciamiento Criminal, comunicará al Ministerio Fiscal aquellos incidentes de seguridad que sean notificados a las autoridades de control, a través de los CSIRT nacionales de referencia, y revistan carácter presuntamente delictivo. En su caso, la Oficina de Coordinación de Ciberseguridad, en el ejercicio de sus funciones, trasladará la información a las Unidades Orgánicas de Policía Judicial correspondientes, de acuerdo con sus respectivas competencias.
4. La Oficina de Coordinación de Ciberseguridad, en el ejercicio de sus funciones, podrá solicitar la identificación de la titularidad real de un activo tecnológico implicado a los proveedores de servicios e internet (ISP) y del mismo modo la información asociada en los registros de nombres de dominio de primer nivel (ccTLD) “.es”.

Artículo 22. *Protección del notificante.*

1. La notificación no implicará una mayor responsabilidad para la entidad.
2. El personal con una relación de servicios con la entidad esencial o importante que participe en la prestación de los servicios de éstas, y que informen sobre incidentes, no podrá ser sancionado o sufrir consecuencias adversas en su puesto de trabajo o en la entidad, salvo en los supuestos en que se acredite mala fe en su actuación y se haya tramitado el correspondiente expediente disciplinario laboral.
3. Se entenderán nulas y sin efecto legal las decisiones del empleador tomadas en perjuicio o detrimento de los derechos laborales de los trabajadores que hayan actuado conforme a este artículo.

Artículo 23. *Obligaciones de información y de colaboración.*

Las entidades esenciales e importantes deberán de suministrar a los CSIRT nacionales de referencia o a las autoridades de control, toda la información que se les requiera para el desempeño de sus funciones. En particular, se les podrá requerir toda la información adicional que sea necesaria para analizar la naturaleza, causas y efectos de los incidentes



notificados y para el cumplimiento de las funciones encomendadas en el ámbito de esta ley.

Artículo 24. Cooperación en lo relativo a los incidentes que afecten a datos personales.

Las autoridades de control cooperarán estrechamente con la Agencia Española de Protección de Datos y, en su caso, con las autoridades independientes de control de las Comunidades Autónomas, para hacer frente a los incidentes que produzcan violaciones de la seguridad de datos personales, y las informará sobre aquellos incidentes que puedan comprometer la seguridad de los datos personales que deban ser objeto de notificación, y su evolución. Todo ello sin perjuicio de las funciones que tienen asignadas los responsables de tratamiento en relación con las notificaciones de las posibles brechas de protección de datos personales conforme a lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales así como, en su caso, 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.

Artículo 25. Autorización para la cesión de datos personales.

Si para realizar notificación de incidentes o su gestión, análisis o resolución es necesario comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso.

Su cesión para estos fines únicamente se entenderá autorizada en los siguientes casos:

- a) De las entidades esenciales e importantes a los CSIRT nacionales de referencia o a las autoridades de control.
- b) Entre los CSIRT nacionales de referencia y las autoridades de control.
- c) Entre los CSIRT nacionales de referencia y los CSIRT designados en otros Estados miembros de la Unión Europea.
- d) Entre los CSIRT nacionales de referencia y otros CSIRT nacionales o internacionales.
- e) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea.

Capítulo IV **Registros de entidades de naturaleza transfronteriza**

Artículo 26. Registro de proveedores de servicios e infraestructuras digitales.

1. El Centro Nacional de Ciberseguridad elaborará y mantendrá un registro con la lista de los proveedores de servicios e infraestructuras digitales. Para ello, las autoridades de control exigirán a los proveedores de servicios de DNS, los registros de nombres de dominio



de primer nivel, las entidades que prestan servicios de registro de nombres de dominio, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados y los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, que presenten la siguiente información:

- a) El nombre de la entidad.
- b) El sector, subsector y tipo de entidad a que se refieren los Anexos I o II, en su caso.
- c) La dirección del establecimiento principal de la entidad y del resto de sus establecimientos legales en la Unión o, de no estar establecida en la Unión, de su representante designado en virtud del artículo 4, apartado 4.
- d) Los datos de contacto actualizados, en particular las direcciones de correo electrónico y los números de teléfono de la entidad y, en su caso, de su representante designado en virtud del artículo 4, apartado 4.
- e) Los Estados miembros en los que la entidad presta servicios, y
- f) Los rangos de IP de la entidad.

2. Asimismo, notificarán cualquier cambio que se produzca en la información remitida sin demora y, en cualquier caso, en el plazo de tres meses desde la fecha en que se produjo el cambio.

3. Tras recibir la información a que se refieren los apartados 1 y 2, salvo la contemplada en el apartado 1 f), el Centro Nacional de Ciberseguridad transmitirá sin demora indebida la información recabada a la ENISA para que la incluya en su registro de entidades. El Centro Nacional de Ciberseguridad podrá acceder al registro, previa solicitud a la ENISA, sin perjuicio de que ésta última adopte, cuando proceda, las medidas para garantizar la confidencialidad de la información.

4. Cuando proceda, la información contemplada en los apartados 1 y 2 se transmitirá de manera segura mediante los mecanismos nacionales implantados a tal efecto.

Artículo 27. *Base de datos sobre el registro de nombres de dominio.*

1. A efectos de contribuir a la seguridad, estabilidad y resiliencia del DNS, los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio recopilarán y mantendrán datos precisos y completos sobre el registro de nombres de dominio en una base de datos de conformidad con lo previsto en la normativa de protección de datos de carácter personal.

2. Para ello, la base de datos sobre el registro de nombres de dominio deberá contener la información necesaria para poder identificar y contactar con los titulares de los nombres de dominio y las entidades que administran los nombres de dominio en los dominios de primer nivel. Dicha información incluirá los elementos siguientes:



- a) El nombre del dominio.
- b) La fecha de registro.
- c) El nombre del solicitante, su dirección de correo electrónico de contacto y su número de teléfono.
- d) La dirección de correo electrónico de contacto y el número de teléfono del punto de contacto que administra el nombre de dominio en caso de que no sean los del solicitante.

3. Los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio deberán desarrollar políticas y procedimientos, incluidos los de verificación, para garantizar que las bases de datos contempladas en el apartado 1 incluyan información precisa y completa. Estas políticas y procedimientos serán públicos.

4. Los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio harán públicos, sin demora indebida, después del registro de un nombre de dominio, aquellos datos del registro que no sean de carácter personal. Asimismo, concederán acceso a datos específicos sobre el registro de nombres de dominio a los solicitantes de acceso legítimos, de conformidad la normativa en materia de protección de datos de carácter personal, previa solicitud lícita y debidamente justificada. La solicitud de acceso deberá resolverse sin demora indebida y, en cualquier caso, en un plazo de setenta y dos horas desde su recepción. Las políticas y los procedimientos de divulgación de dichos datos serán públicos.

5. El cumplimiento de estas obligaciones no podrá implicar la recopilación de datos de registro de nombres de dominio de manera duplicada. A tal fin, los registros de nombres de dominio de primer nivel y a las entidades que prestan servicios de registro de nombres de dominio deberán cooperar entre sí.

Capítulo V **Intercambio de Información**

Artículo 28. Mecanismos de intercambio de información sobre ciberseguridad.

1. Las entidades comprendidas en el ámbito de aplicación de esta ley y, cuando proceda, otras entidades, podrán intercambiar entre sí y de forma voluntaria, información relevante sobre ciberseguridad, en particular la relativa a ciberamenazas, cuasiincidentes, vulnerabilidades, tácticas, técnicas y procedimientos, indicadores de compromiso, información específica del agente de riesgo, alertas de ciberseguridad y recomendaciones sobre configuraciones de las herramientas de seguridad para detectar ciberataques, siempre que dicho intercambio de información:

- a) Se haga con el objetivo de prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión.



- b) Refuerce el nivel de ciberseguridad al concienciar sobre las ciberamenazas, limitar o impedir la propagación, o respaldar un conjunto de capacidades de defensa, corrección y divulgación de las vulnerabilidades, técnicas de detección, contención y prevención de amenazas, estrategias de mitigación, o etapas de respuesta y recuperación, o al fomentar la investigación de ciberamenazas en colaboración con entidades públicas y privadas.

2. El intercambio de información se podrá desarrollar entre comunidades sectoriales o intersectoriales de entidades esenciales e importantes y, cuando proceda, entre sus proveedores o prestadores de servicios, a través de los mecanismos de intercambio de información sobre ciberseguridad que respetarán la posible naturaleza sensible de la información compartida y los derechos fundamentales de las personas.

3. Estos mecanismos de información podrán precisar los elementos operativos, incluido el uso de plataformas de TIC específicas tales como la Red Nacional de Centros de Operaciones de Seguridad, y de herramientas de automatización, incluyendo el contenido y las condiciones de los mecanismos de intercambio de información. Se podrán imponer condiciones a la información que las autoridades de control o los CSIRT nacionales de referencia deben suministrar en estos mecanismos.

4. Las entidades esenciales e importantes notificarán a las autoridades de control su participación en los mecanismos de intercambio de información sobre ciberseguridad en el momento de su incorporación o, en su caso, de su retirada.

Artículo 29. Notificación voluntaria de información pertinente.

1. Sin perjuicio de las obligaciones de notificación previstas en el artículo 18, las entidades esenciales e importantes podrán notificar a las autoridades de control, a través de los CSIRT nacionales de referencia, los incidentes, ciberamenazas y cuasiincidentes que consideren.

Así mismo, las entidades que presten servicios vitales o necesarios para la comunidad y no cumplan los requisitos del artículo 4 para ser consideradas esenciales o importantes podrán notificar los incidentes, ciberamenazas o cuasiincidentes significativos.

Sin perjuicio de la prevención, investigación, detección y enjuiciamiento de infracciones penales, la notificación voluntaria no dará lugar a la imposición a la entidad notificante de obligaciones adicionales a las que no estaría sujeta de no haber presentado dicha notificación.

2. Las notificaciones a las que se refiere el apartado anterior se registrarán por lo dispuesto en este título, y se informará sobre ellas al Centro Nacional de Ciberseguridad.



3. Las notificaciones obligatorias gozarán de prioridad sobre las voluntarias a los efectos de su gestión por los órganos competentes.

Capítulo VI Supervisión y Ejecución

Artículo 30. Aspectos generales relativos a la supervisión de entidades esenciales e importantes.

1. Bajo la superior dirección del Centro Nacional de Ciberseguridad, en su calidad de autoridad nacional competente, las autoridades de control supervisarán y adoptarán las medidas necesarias para garantizar el cumplimiento de la presente ley. Se podrán establecer metodologías de supervisión que permitan priorizar dichas funciones aplicando un enfoque basado en el riesgo.

2. En el ejercicio de las funciones de supervisión se podrá requerir a las entidades esenciales e importantes que proporcionen toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad. Además, podrá solicitar, información sobre la aplicación efectiva de su política de seguridad, así como auditar o exigir a la entidad que someta la seguridad de sus redes y sistemas de información a una auditoría por una entidad de certificación del marco de cumplimiento de seguridad.

En particular, las actuaciones de las autoridades de control tendrán por objeto:

- a) Controlar el cumplimiento de los estándares, guías, especificaciones, instrucciones técnicas, así como cualquier otra disposición que, en su caso, resulten aplicables a las entidades sujetas a su supervisión.
- b) Verificar el cumplimiento de las funciones del responsable de la seguridad de la información designado por las entidades esenciales e importantes.
- c) Realizar las comprobaciones, inspecciones, pruebas y revisiones necesarias para verificar el cumplimiento de las medidas de seguridad.

3. Las entidades esenciales e importantes colaborarán en dicha supervisión, facilitando las actuaciones de inspección, proporcionando toda la información que a tal efecto se les requiera, y aplicando las órdenes o instrucciones dictadas, en su caso, para la subsanación de las deficiencias observadas. Estas medidas también podrán aplicarse a los terceros proveedores de servicios TIC que presten servicios en favor de las entidades supervisadas.

Artículo 31. Medidas de supervisión y ejecución relativas a entidades esenciales.



1. Las medidas de supervisión o ejecución impuestas por las autoridades de control a las entidades esenciales en relación con sus obligaciones serán efectivas, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso individual.
2. Las autoridades de control, en el ejercicio de sus funciones de supervisión, podrán adoptar, al menos, las siguientes medidas en relación con las entidades esenciales:
 - a) Inspecciones in situ y supervisión a distancia, que podrán incluir controles aleatorios realizados por profesionales cualificados.
 - b) Auditorías de seguridad periódicas y específicas llevadas a cabo, cuando resulte de aplicación, por una Entidad de Certificación acreditada del Esquema Nacional de Seguridad. En cualquier otro caso, la evaluación podrá ser realizada por algún organismo de evaluación de la conformidad en materia de ciberseguridad acreditado, conforme a los procedimientos y con la periodicidad que determine normativamente el Centro Nacional de Ciberseguridad. Dichas auditorías de seguridad se basarán en evaluaciones del riesgo, sus resultados se comunicarán a la autoridad de control y al Centro Nacional de Ciberseguridad y sus costes serán sufragados por la entidad auditada, salvo en aquellos casos debidamente motivados en los que el Centro Nacional de Ciberseguridad adopte otra resolución.
 - c) Auditorías extraordinarias, en particular cuando así lo justifique un incidente significativo o un incumplimiento por parte de la entidad esencial.
 - d) Análisis de seguridad basados en criterios de evaluación del riesgo objetivos, no discriminatorios, justos y transparentes, con la cooperación de la entidad afectada cuando sea necesario.
 - e) Solicitudes de información necesaria para evaluar las medidas para la gestión de riesgos de ciberseguridad adoptadas por la entidad afectada, en particular las políticas de ciberseguridad documentadas, así como el cumplimiento de la obligación de presentar información a la autoridad de control.
 - f) Solicitudes de acceso a datos, documentos e información necesaria para el desempeño de sus funciones de supervisión.
 - g) Solicitudes de pruebas de la aplicación de las políticas de ciberseguridad, como por ejemplo los resultados de las auditorías de seguridad realizadas por un auditor cualificado y las correspondientes pruebas subyacentes.
3. En el ejercicio de sus competencias con arreglo al apartado 2, letras e), f) o g), la autoridad de control deberá indicar la finalidad de la solicitud y especificará cuál es la información requerida. En el ejercicio de las funciones de supervisión, la autoridad de control podrá recabar y analizar los Informes de Auditoría y Certificación a los que se haya sometido la entidad.
4. En el ejercicio de sus facultades de ejecución, la autoridad de control podrá, al menos:
 - a) Advertir por incumplimiento a las entidades afectadas.
 - b) Adoptar instrucciones vinculantes, que deberán recoger las medidas necesarias para prevenir o subsanar un incidente, los plazos para ejecutar esas medidas y



notificar su aplicación, o una orden de requerimiento para que las entidades afectadas subsanen las deficiencias o los incumplimientos detectados.

- c) Exigir, en su caso, a las entidades afectadas que pongan fin a las conductas que infrinjan esta norma y que se abstengan de repetirlas.
- d) Exigir a las entidades afectadas que garanticen el cumplimiento de sus medidas para la gestión de riesgos de ciberseguridad o que cumplan las obligaciones de notificación de una manera específica y en un plazo concreto.
- e) Ordenar a las entidades afectadas que informen a las personas físicas o jurídicas a las que prestan servicios o realizan actividades, que puedan verse afectadas por una ciberamenaza significativa sobre la naturaleza de la amenaza, así como sobre cualquier posible medida correctora o de protección que dichas personas puedan adoptar en respuesta a la amenaza.
- f) Ordenar a las entidades afectadas que apliquen las recomendaciones formuladas tras una auditoría de seguridad, en el plazo fijado por la autoridad de control.
- g) Designar un responsable de supervisión para que supervise, durante el periodo que se determine, el cumplimiento por parte de las entidades afectadas de sus obligaciones.
- h) Ordenar a las entidades afectadas que hagan públicos determinados aspectos del incumplimiento de una manera específica.
- i) Ejercer la potestad sancionadora en los casos y términos previstos, así como tramitar en todo caso los procedimientos administrativos derivados de esta ley.

5. Cuando las medidas de ejecución adoptadas con arreglo al apartado 4, letras a), b) c), d) y f), resulten ineficaces para alcanzar los fines previstos por las mismas, la autoridad de control fijará un plazo para que la entidad esencial adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos, sin perjuicio de las responsabilidades que puedan exigirse. Si estas medidas no se adoptan dentro del plazo establecido, la autoridad de control, previa coordinación del Centro Nacional de Ciberseguridad estará facultada para:

- a) Suspender temporalmente, solicitar a una Entidad de Certificación o solicitar autorización a un órgano jurisdiccional, de conformidad con el ordenamiento jurídico, para 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 esencial.
- b) Solicitar que los organismos o los órganos jurisdiccionales competentes de acuerdo con el ordenamiento jurídico prohíban temporalmente a cualquier persona que ejerza responsabilidades de dirección a nivel de director general o de representante legal en dicha entidad esencial ejercer funciones de dirección.

Las suspensiones o las prohibiciones temporales que se impongan se aplicarán únicamente hasta que la entidad afectada adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de la autoridad de control. La imposición de tales suspensiones o



prohibiciones temporales estará sujeta a las garantías adecuadas conforme a los principios generales del ordenamiento jurídico.

Las medidas de ejecución previstas no serán aplicables a las entidades del Sector Público en el ámbito de esta ley.

6. Las personas físicas representantes de las entidades esenciales, así como la autoridad que tenga la competencia para tomar las decisiones en su nombre o ejercer su control, deberá supervisar el cumplimiento de las disposiciones de esta norma, asumiendo, en su caso, la responsabilidad por el incumplimiento de este deber.

7. Cuando se adopte una de las medidas de ejecución contempladas en los apartados 4 o 5, deberán considerarse las mismas circunstancias previstas en el artículo 38.

8. La autoridad de control deberá motivar debidamente las medidas de ejecución que adopte y, con carácter previo a su adopción, notificará sus conclusiones preliminares a las entidades afectadas. También se les concederá un plazo de 15 días para formular alegaciones, salvo en casos debidamente motivados en los que, de otro modo, se obstaculizaría la actuación inmediata para prevenir incidentes o responder a ellos.

9. La autoridad de control informará a las autoridades competentes en materia de protección de entidades críticas cuando ejerza sus facultades de supervisión y ejecución con objeto de garantizar el cumplimiento de esta ley por parte de una entidad identificada como crítica. Cuando proceda, las autoridades competentes en materia de entidades críticas podrán solicitar a la autoridad de control que ejerza sus facultades de supervisión y ejecución respecto a una entidad que esté identificada como entidad crítica.

10. Asimismo, la autoridad de control cooperará con las autoridades designadas con arreglo al Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022. En particular, velará por el cumplimiento de las obligaciones de informe al Foro de Supervisión.

11. El Centro Nacional de Ciberseguridad podrá instar a las autoridades de control el ejercicio de las facultades de supervisión y ejecución respecto a cualquier entidad esencial.

12. Cuando fuera necesario, las autoridades de control podrán recabar el apoyo del CCN-CERT, como CSIRT nacional de referencia de las entidades esenciales, para la ejecución de sus funciones de supervisión y ejecución.

Artículo 32. Medidas de supervisión y ejecución en relación con entidades importantes.

1. Cuando disponga de pruebas, indicios o información de que una entidad importante presuntamente no cumple lo dispuesto en esta ley, la autoridad de control practicará,



cuando proceda, medidas de supervisión a posteriori. Estas medidas deberán ser eficaces, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso.

2. Para el ejercicio de sus funciones de supervisión sobre las entidades importantes, la autoridad de control dispondrá de competencias para acordar, al menos:

- a) Inspecciones in situ y supervisiones a posteriori realizadas a distancia a través de profesionales cualificados.
- b) Auditorías de seguridad periódicas y específicas llevadas a cabo, cuando resulte de aplicación, por una Entidad de Certificación acreditada del Esquema Nacional de Seguridad. En cualquier otro caso, la evaluación podrá ser realizada por algún organismo de evaluación de la conformidad en materia de ciberseguridad acreditado, conforme a los procedimientos y con la periodicidad que determine normativamente el Centro Nacional de Ciberseguridad. Dichas auditorías de seguridad se basarán en evaluaciones del riesgo, sus resultados se comunicarán a la autoridad de control y al Centro Nacional de Ciberseguridad y sus costes serán sufragados por la entidad auditada, salvo en aquellos casos debidamente motivados en los que el Centro Nacional de Ciberseguridad adopte otra resolución.
- c) Análisis de seguridad basados en criterios de evaluación del riesgo objetivos, no discriminatorios, justos y transparentes, con la cooperación de la entidad afectada cuando sea necesario.
- d) Solicitudes de información necesaria para evaluar a posteriori las medidas para la gestión de riesgos de ciberseguridad adoptadas por la entidad afectada, en particular las políticas de ciberseguridad documentadas, así como del cumplimiento de la obligación de presentar información a la autoridad de control.
- e) Solicitudes de acceso a datos, documentos o información necesaria para llevar a cabo sus funciones de supervisión.
- f) Solicitudes de pruebas de la aplicación de las políticas de ciberseguridad, como por ejemplo los resultados de las auditorías de seguridad realizadas por un auditor cualificado y las correspondientes pruebas subyacentes.

Las auditorías de seguridad específicas a que se refiere la letra b) se realizarán de acuerdo con las evaluaciones del riesgo realizadas por la autoridad de control o la entidad auditada.

Los resultados la auditoría de seguridad específicas que se realicen, deberán remitirse a la autoridad de control. Los costes de dicha auditoría de seguridad específica realizada por un organismo independiente serán sufragados por la entidad auditada, salvo en aquellos casos debidamente motivados en los que la autoridad de control decida lo contrario.

En el ejercicio de sus competencias con arreglo a lo dispuesto en las letras d), e) o f) la autoridad de control indicará la finalidad de la solicitud y especificará la información requerida.



3. Para el ejercicio de sus funciones de ejecución en relación con entidades importantes, la autoridad de control dispondrá de competencias para, al menos:

- a) Advertir por el incumplimiento de esta ley a las entidades afectadas.
- b) Adoptar instrucciones vinculantes o una orden de requerimiento para que las entidades afectadas subsanen las deficiencias o los incumplimientos detectados
- c) Ordenar a las entidades afectadas que pongan fin a las conductas que infrinjan la presente ley y que se abstengan de repetirlas.
- d) Ordenar a las entidades afectadas que garanticen que sus medidas para la gestión de riesgos de ciberseguridad son conformes con lo dispuesto en el artículo 15 o que cumplan las obligaciones de notificación establecidas en el artículo 18, de una manera específica y en un plazo concreto.
- e) Ordenar a las entidades afectadas que informen a las personas físicas o jurídicas con respecto a las que prestan servicios o realizan actividades que puedan verse afectadas por una ciberamenaza significativa sobre la naturaleza de la amenaza, así como sobre cualquier posible medida correctora o de protección que dichas personas puedan adoptar en respuesta a la amenaza.
- f) Ordenar a las entidades afectadas que apliquen las recomendaciones formuladas tras una auditoría de seguridad en el plazo normativamente habilitado o, en su defecto, en un plazo razonable.
- g) Ordenar a las entidades afectadas que hagan públicos determinados aspectos del incumplimiento de la presente ley.
- h) Ejercer la potestad sancionadora en los casos y términos previstos, así como tramitar en todo caso los procedimientos administrativos derivados de esta ley.

4. Lo dispuesto en los apartados 6, 7 y 8 del artículo anterior será igualmente de aplicación a las medidas de supervisión y ejecución previstas en este artículo en el caso de las entidades importantes.

5. La autoridad de control cooperará con las autoridades competentes designadas en materia de resiliencia operativa digital del sector financiero con arreglo al Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022. En particular, cuando ejerza sus facultades de supervisión y ejecución al objeto de garantizar el cumplimiento por parte de una entidad importante que sea designada como proveedor tercero esencial de servicios de TIC en virtud de lo previsto en el artículo 31 del Reglamento (UE) 2022/2554, informará al Foro de Supervisión.

6. Cuando fuera necesario, las autoridades de control podrán recabar el apoyo del CSIRT nacional de referencia, para la ejecución de sus funciones de supervisión y ejecución.

Artículo 33. Utilización de esquemas europeos de certificación de la ciberseguridad.

El Centro Nacional de Ciberseguridad, a través de las autoridades de control, instará a las entidades esenciales e importantes para que cumplan cuando proceda, las exigencias



expresadas por los actos de ejecución de la Comisión Europea, en relación con la obligatoriedad de utilizar determinados productos, servicios o procesos de TIC o servicios de seguridad gestionados certificados o a obtener una certificación en virtud de un esquema europeo de certificación de la ciberseguridad en virtud del artículo 49 del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»).

Artículo 34. *Asistencia mutua.*

1. Las funciones de supervisión y ejecución se realizarán en cooperación con las autoridades nacionales competentes de otros Estados miembros de la Unión Europea cuando se refieran a entidades que presten servicios en más de un Estado miembro, o presten servicios en uno o varios Estados miembros y sus redes y sistemas de información estén situados en otro u otros Estados miembros. Dicha cooperación implicará, como mínimo:

- a) La información y consulta a través de los puntos de contacto únicos de las respectivas autoridades nacionales competentes sobre las medidas de supervisión y ejecución adoptadas.
- b) La solicitud de adopción de medidas de supervisión o ejecución entre autoridades nacionales competentes.
- c) La prestación, previa solicitud motivada de las autoridades nacionales competentes de otro Estado miembro, proporcionada a los recursos de los que dispone, de asistencia para que las medidas de supervisión o ejecución puedan aplicarse de manera efectiva, eficiente y coherente.

Esta asistencia mutua podrá abarcar solicitudes de información y medidas de supervisión, incluidas las solicitudes para la realización de inspecciones in situ, supervisión a distancia o auditorías de seguridad específicas.

2. Las solicitudes de asistencia serán obligatorias para las autoridades de control, a menos que carezca de competencias para prestar la asistencia requerida, o que dicha asistencia no se adecúe a sus funciones de supervisión, o la solicitud se refiera a información o implique actividades que, de revelarse o llevarse a cabo, resulten contrarias a intereses esenciales de la seguridad nacional, la seguridad pública o la defensa. Antes de denegar dicha solicitud, a petición de uno de los Estados miembros afectados, el Centro Nacional de Ciberseguridad consultará a la Comisión Europea y a la ENISA.

3. De común acuerdo, las autoridades de control podrán emprender medidas conjuntas de supervisión con las autoridades nacionales competentes de otros Estados miembros.

Capítulo VII **Régimen sancionador**



Sección 1.ª Reglas generales.

Artículo 35. *Sujetos responsables.*

1. La responsabilidad por las infracciones previstas recaerá en las entidades esenciales e importantes autoras del hecho en que consista la infracción.
2. Los miembros de los órganos de dirección de las entidades responderán solidariamente de las infracciones que éstas cometan.

Artículo 36. *Competencia sancionadora.*

La competencia sancionadora corresponderá:

En las infracciones muy graves, a la persona titular del Ministerio Defensa, el Ministerio para la Transformación Digital y de la Función Pública o el Ministerio del Interior respecto de las entidades respectivamente incluidas en el ámbito de competencia de las autoridades de control dependientes de los mismos, previo informe preceptivo del Centro Nacional de Ciberseguridad.

En las infracciones graves y leves, a las autoridades de control designadas según lo previsto en el artículo 7.1 respecto de las entidades incluidas en su respectivo ámbito de competencia.

Artículo 37. *Criterios de graduación de las sanciones.*

Para la determinación de la sanción aplicable en cada caso se tomarán en consideración, además de las recogidas en el artículo 29 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, las siguientes circunstancias:

- a) La naturaleza, gravedad y duración de la infracción o incumplimiento.
- b) El carácter doloso o culposo de la infracción.
- c) La reincidencia, por la comisión en el término de dos años de al menos una infracción de la misma naturaleza, cuando así haya sido declarado por resolución firme en vía administrativa.
- d) El grado de cooperación con las autoridades de control de la entidad esencial o importante.
- e) La ausencia de notificación o subsanación de los incidentes significativos, así como la ausencia de subsanación de deficiencias tras recibir instrucciones vinculantes de las autoridades de control.
- f) El grado de obstrucción de las auditorías o actividades de control ordenadas por la autoridad de control tras la constatación de un incumplimiento.



- g) El suministro de información falsa o manifiestamente imprecisa en relación con las medidas de gestión del riesgo de ciberseguridad o las obligaciones de notificación establecidas.
- h) El perjuicio material o inmaterial causado, incluidas las pérdidas financieras o económicas, los efectos para otros servicios y el número de usuarios afectados.
- i) Las medidas adoptadas por la entidad para prevenir o reducir los daños o perjuicios materiales o inmateriales.
- j) Cualquier adhesión a códigos de conducta o a mecanismos de certificación aprobados.
- k) La naturaleza y el tamaño de la entidad esencial o importante, conforme a lo previsto en el artículo 4.
- l) El grado de responsabilidad de la entidad esencial e importante, teniendo en cuenta las medidas técnicas y organizativas adoptadas para cumplir con la presente ley.
- m) El grado de afectación a la prestación del servicio esencial

Sección 2.ª Infracciones y sanciones

Artículo 38. *Clasificación de las infracciones.*

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

Artículo 39. *Infracciones muy graves.*

Son infracciones muy graves:

- a) La falta de implantación, sin demora indebida, de las medidas técnicas, operativas y de organización determinadas por el Centro Nacional de Ciberseguridad para la gestión de riesgos en la seguridad de las redes y sistemas de información, conforme lo indicado en el artículo 15, cuando dicha omisión haya motivado un incidente significativo.
- b) El incumplimiento reiterado de la obligación de notificar incidentes significativos según se contempla en el artículo 18. Se considerará que es reiterado a partir del segundo incumplimiento.
- c) La falta de adopción de las medidas técnicas, operativas y de organización necesarias para resolver un incidente significativo con arreglo a lo dispuesto en el artículo 17.1.
- d) El incumplimiento en el suministro de la información requerida por la Oficina de Coordinación de Ciberseguridad para determinar el posible carácter delictivo de los incidentes en los términos exigidos por el artículo 21, cuando se hayan perjudicado gravemente el desarrollo de una investigación o cuando se trate de un incumplimiento reiterado. Se considerará que es reiterado a partir del segundo incumplimiento.



- e) El incumplimiento de las obligaciones específicas para garantizar la seguridad de las redes y sistemas de información establecidas por el Centro Nacional de Ciberseguridad en situaciones de justificada necesidad.
- f) El incumplimiento reiterado en el suministro de información requerida por la autoridad de control conforme el artículo 23. Se considerará reiterado a partir del segundo incumplimiento.

Artículo 40. *Infracciones graves.*

Son infracciones graves:

- a) La falta o la demora injustificada en la implantación de las medidas técnicas, operativas y de organización determinadas por el Centro Nacional de Ciberseguridad para la gestión de riesgos en la seguridad de las redes y sistemas de información, conforme lo indicado en el artículo 15.
- b) El impedimento, la obstaculización o la falta de realización de las acciones acordadas por la autoridad de control en el ejercicio de sus funciones de supervisión, conforme a lo dispuesto en los artículos 31.2 y 32.2
- c) El incumplimiento grave de las órdenes o instrucciones vinculantes dictadas por la autoridad de control en ejercicio de funciones de ejecución, así como de los plazos de implantación, previstas en los artículos 31.4, y 32.3.
- d) El incumplimiento, en el plazo concedido al efecto, o el cumplimiento deficiente de las medidas de subsanación o los requisitos exigidos por la autoridad de control a las entidades esenciales conforme a lo previsto en el artículo 30.3, cuando las medidas de ejecución adoptadas conforme al apartado 4 del artículo 31, letras a) a d) y f), resulten ineficaces.
- e) La difusión de información falsa o engañosa al público sobre los estándares que cumple o las certificaciones de seguridad que mantiene en vigor.
- f) El incumplimiento de la obligación de notificar incidentes significativos según se contempla en el artículo 18.
- g) El incumplimiento en el suministro de información requerida por la autoridad de control o el CSRIT nacional de referencia conforme el artículo 23.
- h) El no suministro de la información requerida por la Oficina de Coordinación de Ciberseguridad para determinar el posible carácter delictivo de los incidentes en los términos exigidos por el artículo 21.
- i) La falta de designación de una persona, unidad u órgano colegiado, responsable de la seguridad de la información de conformidad al artículo 16, o que esta carezca de la acreditación exigida, o que se incumplan las disposiciones incluidas en esta norma sobre sus capacidades o funciones dentro de entidad.
- j) El incumplimiento de la obligación prevista en el artículo 31.6, de que las personas físicas con facultades de representación o para la toma de decisiones o ejercer el control sobre la misma tengan competencia para velar por el cumplimiento de esta norma y, en su caso, puedan ser consideradas responsables por el incumplimiento de sus deberes en el marco de esta ley.



- k) El incumplimiento de las obligaciones establecidas en el artículo 4.4 de comunicar la inclusión en la lista de las entidades esenciales e importantes o de autorregistro, en su caso, o de remitir la información prevista en el mismo.
- l) El incumplimiento de las obligaciones de remisión de información exigidas conforme el artículo 26.1, así como la remisión fuera del plazo marcado en el artículo 26.2.
- m) El incumplimiento en la recopilación y mantenimiento de datos precisos y completos sobre el registro de nombres de dominio reflejado en el artículo 27.
- n) La no solicitud de ayuda especializada al CSIRT nacional de referencia, cuando la entidades esenciales e importantes no puedan resolver por sí mismas los incidentes.

Artículo 41. *Infracciones leves.*

Son infracciones leves:

- a) El incumplimiento leve de las órdenes o instrucciones vinculantes dictadas por la autoridad de control en ejercicio de funciones de ejecución, así como de los plazos de implantación, previstas en los artículos 31.4, y 32.3.
- b) El cumplimiento de la obligación de notificar incidentes significativos sin recoger la información que deben reunir los diferentes informes de notificación de incidentes teniendo en cuenta lo dispuesto en el artículo 18.
- c) La remisión de información incompleta, inexacta o con dilación indebida a la autoridad de control o al CSIRT nacional de referencia de acuerdo con lo establecido en el artículo 23.
- d) La falta de información a las personas físicas o jurídicas a las que presta servicios o respecto de las que realiza actividades, que puedan verse afectadas por una ciberamenaza significativa, acerca de la naturaleza de la amenaza, así como sobre cualquier posible medida correctora o de protección que dichas personas puedan adoptar en respuesta a la misma.
- e) El incumplimiento de la obligación de informar en plazo a la autoridad de control respectiva de la designación del responsable de la seguridad de la información, así como los nombramientos y ceses posteriores que se produzcan.
- f) El incumplimiento de las obligaciones de formación a los empleados y órganos de dirección incluidas en esta ley.
- g) La comunicación de los datos recogidos en el artículo 4.4 de forma incompleta o inexacta, o el incumplimiento del deber de comunicar cualquier cambio en la información remitida en la forma y plazos previstos en dicho artículo.

Artículo 42. *Sanciones.*

1. Las infracciones muy graves se sancionarán con multa de 500.001 hasta 2.000.000 euros.



No obstante, las infracciones muy graves recogidas en el artículo 39 letras a y b cometidas por una entidad esencial podrán sancionarse con multa de hasta 10.000.000 euros o una cuantía equivalente al 2% del volumen de negocios anual total a nivel mundial de la empresa a la que pertenece la entidad esencial durante el ejercicio financiero anterior, optándose por la de mayor cuantía.

Las infracciones muy graves recogidas en el artículo 39 letras a y b cometidas por una entidad importante, podrán sancionarse con multa de hasta 7.000.000 euros o una cuantía equivalente al 1,4% del volumen de negocios anual total a nivel mundial de la empresa a la que pertenece la entidad importante durante el ejercicio financiero anterior, optándose por la de mayor cuantía.

2. Las infracciones graves se sancionarán con multa de 100.001 € hasta 500.000 euros.

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

4. La multa impuesta por la comisión de infracciones muy graves y graves podrá llevar aparejada la sanción accesoria de amonestación pública en el «Boletín Oficial del Estado», que indicará la persona responsable y el carácter de la infracción.

Artículo 43. *Infracciones del Sector Público.*

1. Las infracciones cometidas por órganos, organismos o entidades del Sector Público no serán objeto de sanción. No obstante, el órgano competente para sancionar acordará mediante resolución las medidas que estime oportunas para que cesen y se corrijan los efectos de la infracción. Esta resolución se notificará al órgano o entidad infractora y a los afectados, si los hubiera.

Además de lo anterior, el órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran.

2. Se comunicarán al órgano sancionador las resoluciones que se adopten en cumplimiento de las medidas a las que se refiere el apartado anterior.

Sección 3.ª Procedimiento sancionador

Artículo 44. *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, de Régimen Jurídico del Sector Público, sin perjuicio de las especialidades que se regulan en este capítulo.

Artículo 45. *Concurrencia de infracciones.*



1. No podrán sancionarse hechos que ya hayan sido sancionados penal o administrativamente cuando se aprecie identidad de sujeto, de hecho y de 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 los mismos a los órganos u organismos competentes a los efectos de iniciar, en su caso, el oportuno procedimiento sancionador.

Artículo 46. Subordinación del procedimiento administrativo sancionador respecto del penal.

1. Los hechos declarados probados por resoluciones judiciales penales firmes vincularán al órgano administrativo respecto de los procedimientos sancionadores que substancien por los mismos hechos.
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 47. *Medidas provisionales.*

Se podrán adoptar medidas provisionales de conformidad con el artículo 56 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.

Las autoridades de control estarán facultadas para fijar un plazo en el que la entidad esencial 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 de control estarán facultadas para:

- a) Suspender temporalmente o solicitar a un 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 esencial.
- b) Solicitar que los organismos o los órganos jurisdiccionales competentes de acuerdo con el ordenamiento jurídico prohíban temporalmente ejercer sus funciones a cualquier



persona que ejerza responsabilidades de dirección a nivel de director general o representante legal en dicha entidad esencial.

3. Las medidas provisionales previstas no serán aplicables a las entidades del Sector Público sujetas a esta ley.

Artículo 48. Caducidad del procedimiento.

1. El procedimiento caducará transcurridos seis meses desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concorra identidad de sujeto, hecho y fundamento, hasta la finalización de éste.

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.

Artículo 49. Prescripción de las infracciones.

1. Las infracciones administrativas tipificadas en esta ley prescribirán a los seis meses, al año o a los dos años de haberse cometido, según sean leves, graves o muy graves, respectivamente.

2. Los plazos señalados en esta ley 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 la del último acto con que la infracción se consumó.

3. Interrumpirá la prescripción la iniciación, con conocimiento de la persona interesada, del procedimiento sancionador, reanudándose el cómputo del plazo de prescripción si el procedimiento estuviera paralizado más de un mes por causa no imputable a la persona presuntamente responsable.

4. Se interrumpirá, igualmente, la prescripción como consecuencia de la apertura 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.



Artículo 50. 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 infracciones leves al año, computados desde el día siguiente a aquel en que adquiera firmeza en vía administrativa la resolución por la que se impone la sanción.
2. Interrumpirá la prescripción la iniciación, con conocimiento de la persona interesada, del procedimiento de ejecución, volviendo a transcurrir el plazo si aquél se paraliza durante más de un mes por causa no imputable a la persona infractora.

Disposición adicional primera. Centro Nacional de Ciberseguridad

El Gobierno aprobará, en el plazo máximo de doce meses desde la entrada en vigor de la presente ley, el Real decreto por el que se determine el rango, carácter y estructura administrativa del Centro Nacional de Ciberseguridad, adscrito al Gabinete de la Presidencia del Gobierno, dirigiendo y coordinando bajo una autoridad única el ejercicio de las competencias estatales previstas en esta ley.

Asumirá además cualesquiera otras funciones que se le encomienden en el ámbito de la ciberseguridad nacional, sin perjuicio de las competencias legalmente reservadas a otros organismos e instituciones.

Disposición adicional segunda. Régimen específico del Banco de España.

Las disposiciones de esta ley se entenderán sin perjuicio de las competencias y funciones atribuidas al Banco de España, al Banco Central Europeo y al Sistema Europeo de Bancos Centrales, de conformidad con el Tratado de Funcionamiento de la Unión Europea, los Estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo, el Reglamento (UE) 1024/2013 del Consejo, de 15 de octubre de 2013, que encomienda al Banco Central Europeo tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito y la Ley 13/1994, de 1 de junio, de Autonomía del Banco de España.

Disposición adicional tercera. Información sobre incidentes en el sistema financiero.

Las autoridades de control y los CSIRT nacionales de referencia informarán al titular de la Secretaría de Estado de Economía y Apoyo a la Empresa, a través de la Secretaría General del Tesoro y Financiación Internacional, sobre aquellos incidentes que puedan tener efectos significativos en los servicios esenciales del sistema financiero.

A estos efectos, se entenderá que tienen efectos significativos cuando su umbral o nivel de impacto sea crítico, muy alto o alto, según lo señalado en las instrucciones y guías de



comunicación de incidentes, entre ellas la Instrucción Nacional de Notificación y Gestión de ciberincidentes contenida como Anexo en el Real Decreto 43/2021 de 26 de enero, de seguridad de las redes y sistemas de información.

Disposición adicional cuarta. Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

La Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes recogida en el artículo 19 de esta ley, será la plataforma común prevista en el artículo 19.4 del Real Decreto-ley 12/2018 y desarrollada por el artículo 11 del Real Decreto 43/2021.

Disposición adicional quinta. *Base de datos de incidencias de seguridad que revistan carácter de delito.*

1. La Dirección General de Coordinación y Estudios, de la Secretaría de Estado de Seguridad, será el órgano responsable del tratamiento denominado base de datos de incidencias de seguridad que revistan carácter de delito.
2. La finalidad que persigue el tratamiento es la utilización de los datos obtenidos en la gestión, seguimiento y resolución de incidentes de ciberseguridad que afecten a entidades esenciales o importantes, cuando puedan entenderse presuntamente delictivos.
3. Se podrán tratar, al menos, los datos relativos a la identidad de las personas, datos identificativos de terminales y dispositivos de conectividad y los datos personales de identidad y contacto de los responsables, gestores y usuarios del fichero del tratamiento.
4. Serán destinatarios de los datos los órganos jurisdiccionales del orden penal, el Ministerio Fiscal y las Fuerzas y Cuerpos de Seguridad, así como otras entidades cuando se prevea legalmente.

Los destinatarios serán también responsables del tratamiento de los datos que les hubieran comunicado conforme a las disposiciones de esta ley.

5. La base jurídica principal del tratamiento de acuerdo con el objetivo y finalidad de la presente ley es el cumplimiento de acuerdo con lo dispuesto en el artículo 11 y 13 de 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, 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.



La base jurídica aplicable a las transferencias de datos personales a terceros países u organizaciones internacionales se adecuará a lo dispuesto en los artículos 43 a 47 de la Ley Orgánica 7/2021, de 26 de mayo.

6. Solo se recogerán los datos necesarios para el cumplimiento de las finalidades establecidas, de acuerdo con el principio de minimización de datos.

7. 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.

8. 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 transcurrido dicho periodo de conservación, los datos serán suprimidos de manera que se imposibilite la correlación o identificación de estos con los interesados.

9. Los responsables del tratamiento deberán garantizar la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta, en todo caso, lo prevenido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

10. El ejercicio de derechos para las personas físicas sujetas a la normativa de protección de datos se garantizará conforme a dicha normativa. Serán atendidas las solicitudes 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 y el momento procesal correspondiente.

En función de la posible fase procesal o situación del tratamiento en la que encuentren los datos, con el fin de que no se obstaculicen las investigaciones y evitar perjuicios sobre la detección, investigación y enjuiciamiento de las infracciones, el responsable del tratamiento obrará conforme al artículo 26 de la Ley Orgánica 7/2021, de 26 de mayo o restringirá los derechos de acceso, rectificación, limitación y supresión respecto al tratamiento de datos en el fichero.

Esta restricción afectará al contenido de la información a facilitar en caso de que se solicite el ejercicio de alguno de esos derechos, sustituyéndose en función del supuesto, por una redacción neutra o por una que informe sobre la existencia de la restricción, las razones de esta y la posibilidad de presentar una reclamación ante la autoridad de protección de datos. La información se facilitará de conformidad con lo establecido en el artículo 24 de la Ley Orgánica 7/2021, de 26 de mayo, en el plazo de un mes prorrogable por otros dos desde la



recepción de la solicitud y a través de los medios que el interesado hubiese utilizado para efectuarla. El responsable del tratamiento documentará los fundamentos de hecho y de derecho en los que se sustente la decisión denegatoria del ejercicio del derecho. Dicha información estará a disposición de las autoridades de protección de datos.

Si como consecuencia del tratamiento de los datos personales se incoara un procedimiento penal, deberá cumplirse con el deber de información en los términos previstos en la Ley de Enjuiciamiento Criminal.

Disposición adicional sexta. Salvaguarda de intereses y funciones estatales esenciales.

1. Las obligaciones establecidas no implicarán el suministro de información cuya divulgación sea contraria a los intereses esenciales de España en materia de la Seguridad Nacional, la seguridad pública o la Defensa Nacional. La información que se considere confidencial de acuerdo con el ordenamiento jurídico de la Unión Europea o nacional, se intercambiará con la Comisión y otras autoridades competentes únicamente cuando sea necesario a efectos de la aplicación de esta ley, y se limitará a aquella información que resulte pertinente y proporcionada para la finalidad del intercambio. En todo caso, se preservará la confidencialidad, la seguridad y los intereses comerciales de las entidades interesadas.

2. Lo dispuesto en esta ley se entenderá sin perjuicio de la normativa relativa al ejercicio de las competencias para la salvaguarda de la seguridad nacional y la defensa, así como de otras funciones esenciales del Estado, entre las que se incluyen la gestión de los procesos electorales y consultas directas al electorado, el mantenimiento de la seguridad pública, la información clasificada, y la prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Disposición adicional séptima. *Representación en el Centro Europeo de Competencia Industrial.*

Bajo la supervisión y dirección del Centro Nacional de Ciberseguridad, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales del Ministerio para la Transformación Digital y de la Función Pública, asumirá la representación de España en el Consejo de Administración del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad, establecido por el Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021. Asimismo, el Instituto Nacional de Ciberseguridad, ejercerá como Centro Nacional de Coordinación a los efectos de dicho reglamento, bajo la supervisión y dirección del Centro Nacional de Ciberseguridad.

Disposición adicional octava. *Autoridad Nacional de Certificación de la Ciberseguridad.*

1. De acuerdo con el artículo 58(1) Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la



Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº526/2013 («Reglamento sobre la Ciberseguridad») y con lo dispuesto en los artículos 1 y 2.2.c del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, el director de dicho organismo será la autoridad nacional de certificación de la ciberseguridad.

2. La Autoridad Nacional de Certificación de la Ciberseguridad tendrá las funciones y competencias incluidas en el artículo 58(7 y 8) de citado reglamento europeo.

3. Se faculta a la Autoridad Nacional de Certificación de la Ciberseguridad para que dicte las disposiciones necesarias para el correcto funcionamiento a nivel nacional de los esquemas de certificación europeos que se establezcan.

4. En todo aquello relativo a la aplicación de la presente ley, la Autoridad Nacional de Certificación de la Ciberseguridad ejercerá sus funciones, competencias y facultades bajo la supervisión y dirección del Centro Nacional de Ciberseguridad.

Disposición transitoria primera. *Obligaciones de comunicación.*

1. El Consejo Nacional de Ciberseguridad, a través de la Comisión Permanente de Ciberseguridad, como grupo de trabajo de apoyo al Consejo, presidida por el Departamento de Seguridad Nacional, notificará, antes del 17 de abril de 2025:

- a) A la Comisión y al Grupo de Cooperación de la Unión Europea, el número de entidades esenciales e importantes respecto de cada sector y subsector a que se refieren los anexos I o II, y
- b) A la Comisión, la información pertinente sobre el número de entidades esenciales e importantes identificadas, el sector y subsector señalados en los anexos I o II a los que pertenecen, el tipo de servicio que prestan y la disposición en virtud de la cual fueron identificados.

Estas notificaciones se actualizarán posteriormente cada dos años a través del Centro Nacional de Ciberseguridad.

Se podrán notificar a la Comisión, a petición de esta y antes del 17 de abril de 2025, los nombres de las entidades esenciales e importantes a que se refiere la letra b).

2. El Consejo Nacional de Ciberseguridad, a través del Departamento de Seguridad Nacional, previa aprobación en la Comisión permanente de ciberseguridad, en el plazo de tres meses desde la entrada en vigor de esta ley, notificará a la Comisión Europea la identidad de su autoridad de gestión de crisis de ciberseguridad y cualquier modificación posterior de esta.



3. El Consejo Nacional de Ciberseguridad, a través del Departamento de Seguridad Nacional previa aprobación en la Comisión permanente de ciberseguridad, en un plazo de tres meses a partir de su adopción, presentará a la Comisión Europea y a la red europea de organizaciones de enlace para las crisis de ciberseguridad EU-CyCLONe la información pertinente relativa a los requisitos del Plan de Respuesta a Incidentes y Crisis de Ciberseguridad a gran escala, pudiendo excluir información cuando y en la medida en que sea necesario para la seguridad nacional.

4. El Consejo Nacional de Ciberseguridad, a través del Departamento de Seguridad Nacional, previa aprobación en la Comisión permanente de ciberseguridad notificará sin dilación indebida a la Comisión Europea la identidad de los CSIRT nacionales referencia designados en virtud del artículo 10, y cualquier cambio en lo notificado que se introduzca posteriormente.

Disposición transitoria segunda. *Registro de entidades.*

1. El Consejo Nacional de Ciberseguridad, a través de la Comisión permanente de ciberseguridad como grupo de trabajo de apoyo al Consejo, presidida por el departamento de Seguridad Nacional elaborará la lista de entidades esenciales e importantes referida en el artículo 4.3 antes del 17 de abril de 2025, utilizando para ello la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

2. Asimismo, los proveedores de servicios e infraestructuras digitales referenciados en el artículo 26.1, deben presentar, ante la autoridad de control, los datos recogidos en el artículo 28, antes del 17 de enero de 2025.

Disposición transitoria tercera. *Régimen transitorio.*

1. Hasta que inicie sus actividades el Centro Nacional de Ciberseguridad, conservarán transitoriamente su vigencia las disposiciones del Real Decreto-ley 12/2018, de 7 de septiembre, y del Real Decreto 43/2021, de 26 de enero, relativas a las autoridades competentes, CSIRT nacionales de referencia y punto de contacto único.

2. Hasta la modificación, sustitución o derogación de la Instrucción Nacional de Notificación y Gestión de Ciberincidentes, se considerarán incidentes significativos aquellos que puedan categorizarse con un nivel de peligrosidad o impacto alto, muy alto o crítico, conforme a lo establecido en dicha Instrucción.

3. Hasta la creación del Centro Nacional de Ciberseguridad, no será preceptiva la emisión del informe exigido en el artículo 36 en los procedimientos sancionadores por infracciones muy graves.

Disposición derogatoria única. *Derogación normativa.*



1. Quedan derogadas las siguientes disposiciones:

a) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

b) Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, con la excepción de la Instrucción nacional de notificación y gestión de ciberincidentes contenida en su anexo, que seguirá vigente en tanto no sea expresamente modificada, sustituida o derogada expresamente.

2. Asimismo quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta ley.

Disposición final primera. *Título competencial.*

Esta Ley se dicta al amparo de lo previsto en el artículo 149.1. 21.^ª y 29.^ª de la Constitución Española, que atribuyen respectivamente al Estado competencia exclusiva en materia de régimen general de telecomunicaciones y de seguridad pública.

Disposición final segunda. *Modificación de la Ley 5/2014, de 4 de abril, de Seguridad Privada.*

Se modifica el apartado 2 del artículo 3 de la Ley 5/2014, de 4 de abril, de Seguridad Privada, que queda redactado como sigue:

“2. Igualmente, en la medida que resulte pertinente en cada caso, se aplicarán a los establecimientos obligados a disponer de medidas de seguridad, a los usuarios de los servicios de seguridad privada, a los ingenieros y técnicos que desarrollen las tareas que les asignan esta ley, operadores de seguridad, el personal que realice tareas de ciberseguridad en los casos que legal o reglamentariamente se determine, a los profesores de centros de formación, a las empresas prestadoras de servicios de seguridad informática, a las centrales receptoras de alarmas de uso propio y a los centros de formación de personal de seguridad privada”.

Se modifica el apartado 9 del artículo 2 de la Ley 5/2014, de 4 de abril, de Seguridad Privada, que queda redactado como sigue:

“9. Personal acreditado: profesores de centros de formación, ingenieros y técnicos que desarrollen las tareas que les asignan esta ley; operadores de seguridad; y el personal que realice tareas de ciberseguridad en los casos que legal o reglamentariamente se determine.”

Disposición final tercera. *Desarrollo reglamentario.*



Se habilita a los titulares de los Ministerios de Defensa, Interior y para la Transformación Digital y de la Función Pública, así como a los titulares de los Ministerios y organismos relacionados en el artículo 7, para dictar, en el ámbito de sus respectivas competencias, las disposiciones necesarias para el desarrollo y aplicación de lo previsto en esta ley.

Disposición final cuarta. *Incorporación al derecho de la Unión Europea.*

Esta ley incorpora al derecho español 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) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Disposición final quinta. *Entrada en vigor.*

Esta ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».



ANEXO I

SECTORES DE ALTA CRITICIDAD

Sector		Subsector		Tipo de entidad	Punto de contacto sectorial
1.	Energía	a)	Electricidad	Empresas eléctricas, tal como se definen en el artículo 2, punto 57, de la Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo (1), que efectúan la función de «suministro», tal como se define en el artículo 2, punto 12, de dicha Directiva	Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.
				Gestores de la red de distribución, tal como se definen en el artículo 2, punto 29, de la Directiva (UE) 2019/944	
				Gestores de la red de transporte, tal como se definen en el artículo 2, punto 35, de la Directiva (UE) 2019/944	
				Productores, tal como se definen en el artículo 2, punto 38, de la Directiva (UE) 2019/944	
				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 (2)	
				Participantes en el mercado de la electricidad, tal como se definen en el artículo 2, punto 25, del Reglamento (UE) 2019/943 que presten servicios de agregación, respuesta de demanda o almacenamiento de energía, tal como se define en el artículo 2, puntos 18, 20 y 59, de la Directiva (UE) 2019/944	



		Operadores de un punto de recarga que sean responsable de la gestión y explotación de un punto de recarga, que presta un servicio de recarga al usuario final también en nombre y por cuenta de un proveedor de servicios de movilidad
b)	Sistemas urbanos de calefacción y de refrigeración	Operadores de sistemas urbanos de calefacción o de refrigeración, tal como se definen en el artículo 2, punto 19, de la Directiva (UE) 2018/2001 del Parlamento Europeo y del Consejo (3)
c)	Crudo	Operadores de oleoductos de transporte de crudo
		Operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte
		Entidades centrales de almacenamiento, tal como se definen en el artículo 2, letra f), de la Directiva 2009/119/CE del Consejo (4)
d)	Gas	Empresas suministradoras de gas, tal como se definen en el artículo 2, punto 8, de la Directiva 2009/73/CE del Parlamento Europeo y del Consejo (5)
		Gestores de la red de distribución, tal como se definen en el artículo 2, punto 6, de la Directiva 2009/73/CE
		Gestores de la red de transporte, tal como se definen en el artículo 2, punto 4, de la Directiva (UE) 2009/73/CE
		Gestores de almacenamientos, tal como se definen en el artículo 2, punto 10, de la Directiva 2009/73/CE
		Gestores de la red de GNL, tal como se definen en el artículo 2, punto 12, de la Directiva 2009/73/CE
		Compañías de gas natural, tal como se definen en el artículo 2, punto 1, de la Directiva 2009/73/CE



				Operadores de instalaciones de refinado y tratamiento de gas natural	
		e)	Hidrógeno	Operadores de producción, almacenamiento y transporte de hidrógeno	
2.	Transporte	a)	Transporte aéreo	Compañías aéreas, tal como se definen en el artículo 3, punto 4, del Reglamento (CE) n.o 300/2008 utilizadas con fines comerciales	Ministerio de Transportes, Movilidad y Agenda Urbana, a través de la Secretaría de Estado de Transportes, Movilidad y Agenda Urbana.
				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 (6); aeropuertos, tal como se definen en el artículo 2, punto 1, de dicha Directiva, en particular los aeropuertos de la red básica enumerados en el anexo II, sección 2, del Reglamento (UE) n.o 1315/2013 del Parlamento Europeo y del Consejo (7); y entidades que explotan instalaciones anexas dentro de los recintos de los aeropuertos	
				Operadores de control de la gestión del tráfico que prestan servicios de control del tránsito aéreo, tal como se definen en el artículo 2, punto 1, del Reglamento (CE) n.o 549/2004 del Parlamento Europeo y del Consejo (8)	
		b)	Transporte por ferrocarril	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 (9)	
				Empresas ferroviarias, tal como se definen en el artículo 3, punto 1, de la Directiva 2012/34/UE, incluidos los explotadores de instalaciones de servicio, tal como se definen en el artículo 3, punto 12 de dicha Directiva	



		c)	Transporte marítimo y fluvial	<p>Empresas de transporte marítimo, fluvial y de cabotaje, tanto de pasajeros como de mercancías, tal como se definen para el transporte marítimo en el anexo I del Reglamento (CE) n.o 725/2004 del Parlamento Europeo y del Consejo (10), sin incluir los buques particulares explotados por esas empresas</p> <p>Organismos gestores de los puertos, tal como se definen en el artículo 3, punto 1, de la Directiva 2005/65/CE del Parlamento Europeo y del Consejo (11), incluidas sus instalaciones portuarias, tal como se definen en el artículo 2, punto 11, del Reglamento (CE) n.o 725/2004, y entidades que operan obras y equipos que se encuentran en los puertos</p> <p>Operadores de servicios de tráfico de buques (STB), tal como se definen en el artículo 3, letra o), de la Directiva 2002/59/CE del Parlamento Europeo y del Consejo (12)</p>	
		d)	Transporte por carretera	<p>Autoridades viarias, tal como se definen en el artículo 2, punto 12, del Reglamento Delegado (UE) 2015/962 de la Comisión (13) 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 sea una parte no esencial de su actividad general</p> <p>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 (14)</p>	
3.	Banca			Entidades de crédito, tal como se definen en el artículo 4, punto 1, del Reglamento (UE) n.o 575/2013 del Parlamento Europeo y del Consejo (15)	El Banco de España



4.	Infraestructuras de los mercados financieros	Gestores de centros de negociación, tal como se definen en el artículo 4, punto 24, de la Directiva 2014/65/UE del Parlamento Europeo y del Consejo (16)	La Comisión Nacional del Mercado de Valores.
		Entidades de contrapartida central (ECC), tal como se definen en el artículo 2, punto 1, del Reglamento (UE) n.o 648/2012 del Parlamento Europeo y del Consejo (17)	La Comisión Nacional del Mercado de Valores.
5.	Sector sanitario	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 (18)	Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.
		Laboratorios de referencia de la UE, tal como se definen en el artículo 15, del Reglamento (UE) .../...del Parlamento Europeo y del Consejo (19)	
		Entidades que realizan actividades de investigación y desarrollo de medicamentos, tal como se definen en el artículo 1, punto 2, de la Directiva 2001/83/CE del Parlamento Europeo y del Consejo (20)	
		Entidades que fabrican productos farmacéuticos de base y especialidades farmacéuticas a que se refiere la sección C, división 21, de la NACE Rev. 2	
		Entidades que fabrican productos sanitarios que se consideran esenciales en situaciones de emergencia de salud pública («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 (21)	



6.	Agua potable		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 (22), excluidos los distribuidores para los que la distribución de aguas destinadas al consumo humano sea una parte no esencial de su actividad general de distribución de otros bienes y productos básicos	Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Medio Ambiente.
7.	Aguas residuales		Empresas dedicadas a la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales, tal como se definen en el artículo 2, puntos 1 a 3, de la Directiva 91/271/CEE del Consejo (23), excluidas las empresas para las que la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales sea una parte no esencial de su actividad general	Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Medio Ambiente.
8.	Infraestructura digital		Proveedores de puntos de intercambio de internet	Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
			Proveedores de servicios de DNS, excluidos los operadores de servidores raíz	
			Registros de nombres de dominio de primer nivel	
			Proveedores de servicios de computación en nube	
			Proveedores de servicios de centro de datos	
			Proveedores de redes de distribución de contenidos	
			Prestadores de servicios de confianza	
			Proveedores de redes públicas de comunicaciones electrónicas	
Proveedores de servicios de comunicaciones electrónicas disponibles para el público				



9.	Gestión de servicios de TIC (de empresa a empresa)		Proveedores de servicios gestionados	Ministerio de Transformación Digital y la Función Pública, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
			Proveedores de servicios de seguridad gestionados	
10.	Entidades de la Administración pública, con exclusión del poder judicial, los parlamentos y los bancos centrales		Entidades de la Administración pública central, tal como se definen en el Estado miembro con arreglo a las disposiciones del Derecho nacional	Ministerio de Defensa, a través del Centro Criptológico Nacional
			Entidades de la Administración pública a escala regional, según su definición en el Estado miembro con arreglo a las disposiciones del Derecho nacional	
11.	Espacio		Operadores de infraestructuras terrestres, cuya propiedad, gestión y explotación descansa en los Estados miembros o en entidades privadas, que apoyan la prestación de servicios espaciales, excepto los proveedores de redes públicas de comunicaciones electrónicas	Ministerio de Defensa y Ministerio de Ciencia, Innovación y Universidades, a través de la Agencia Espacial Española
12.	Industria Nuclear		Centrales nucleares y entidades relacionadas con la utilización, producción, almacenamiento y transporte de mercancías y materiales nucleares o radiológicos	1.º El Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.
				2.º El Consejo de Seguridad Nuclear.



MINISTERIO
DEL INTERIOR



ANEXO II

OTROS SECTORES

Sector		Subsector	Tipo de entidad	Punto de contacto sectorial
1.	Servicios postales y de mensajería		Proveedores de servicios postales, tal como se definen en el artículo 2, punto 1 bis, de la Directiva 97/67/CE, incluidos los proveedores de servicios de mensajería	Ministerio de Transportes, Movilidad y Agenda Urbana, a través de la Subsecretaría de Transportes y Movilidad sostenible
2.	Gestión de residuos		Empresas que realizan la gestión de residuos, tal como se definen en el artículo 3, punto 9, de la Directiva 2008/98/CE del Parlamento Europeo y del Consejo (1), excepto aquellas para las que la gestión de residuos no es su principal actividad económica	Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Medio Ambiente.
3.	Fabricación, producción y distribución de sustancias y mezclas químicas		Empresas que realizan la fabricación de sustancias y la distribución de sustancias o mezclas, tal como se definen en el artículo 3, puntos 9 y 14, del Reglamento (CE) n.o 1907/2006 del Parlamento Europeo y del Consejo (2) y empresas que realizan la producción de artículos, tal como se definen en el artículo 3, punto 3, de dicho Reglamento, a partir de sustancias y mezclas	Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.



4.	Producción, transformación y distribución de alimentos		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 (3), que se dediquen a la distribución al por mayor y a la producción y transformación industriales	<p>1.º El Ministerio de Agricultura, Pesca y Alimentación, a través de la Secretaría General de Recursos Agrarios y Seguridad Alimentaria.</p> <p>2.º El Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.</p> <p>3.º El Ministerio de Industria, Comercio y Turismo, a través de la Secretaría de Estado de Comercio.</p> <p>4.º El Ministerio de Derechos Sociales, Consumo y Agenda 2030, a través del Centro Nacional de Seguridad Alimentaria y Nutrición (AESAN).</p>	
5.	Fabricación	a)	Fabricación de productos sanitarios y productos sanitarios para diagnóstico in vitro	Entidades que fabrican los productos sanitarios, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo (4), y entidades que fabrican los productos sanitarios para diagnóstico in vitro, tal como se definen en el artículo 2, punto 2, del Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo (5), excepto las entidades que fabrican productos sanitarios a que se refiere el anexo I, punto 5, quinto guion, de la presente Directiva	Ministerio de Industria, Comercio y Turismo, a través de _____



		b)	Fabricación de productos informáticos, electrónicos y ópticos	Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 26, de la NACE Rev. 2	
		c)	Fabricación de material eléctrico	Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 27, de la NACE Rev. 2	
		d)	Fabricación de maquinaria y equipo n.c.o.p.	Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 28, de la NACE Rev. 2	
		e)	Fabricación de vehículos de motor, remolques y semirremolques	Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 29, de la NACE Rev. 2	
		f)	Fabricación de otro material de transporte	Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 30, de la NACE Rev. 2	
6.	Proveedores de servicios digitales			Proveedores de mercados en línea	Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado
				Proveedores de motores de búsqueda en línea	



MINISTERIO
DEL INTERIOR

			Proveedores de plataformas de servicios de redes sociales	de Telecomunicaciones e Infraestructuras Digitales.
7.	Investigación		Organismos de investigación	Ministerio de Ciencia e Innovación, a través de la Secretaría General de Investigación
8.	Seguridad Privada		Empresas de seguridad privada y despachos de detectives conforme lo recogido en la Ley 5/2014, de 4 de abril, de Seguridad Privada.	Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.