MEMORIA DEL ANÁLISIS DE IMPACTO NORMATIVO DEL ANTEPROYECTO DE LEY DE COORDINACIÓN Y GOBERNANZA DE LA CIBERSEGURIDAD

1. FICHA DEL RESUMEN EJECUTIVO

Ministerios / Órganos proponentes	• Ministerio del Interior • Presidencia del Gobierno • Ministerio de Defensa. • Ministerio para la Transformación Digital y de la Función Pública.	**Fecha**	Noviembre 2024
Título de la norma	Ley de coordinación y gobernanza de la ciberseguridad		
Tipo de memoria	☑ Normal ☐ Abreviada		
OPORTUNIDAD DE LA PROPUESTA			
Situación que se regula	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.		
Objetivos que se persiguen	- Crear una Autoridad Nacional Competente única en materia de ciberseguridad. - Definir un criterio uniforme para determinar las entidades que están incluidas en el ámbito de aplicación clasificadas en entidades esenciales y entidades importantes. - Establecer un catálogo de medidas necesarias para la gestión de riesgos de ciberseguridad. - Reforzar el procedimiento de notificación de incidentes que perturben o puedan perturbar la prestación de los servicios de entidades esenciales e importantes. - Crear la figura del responsable de seguridad de la información. - Reforzar las normas relativas al intercambio de información sobre ciberseguridad. - Establecer un marco institucional y de coordinación entre las autoridades competentes.		

Principales alternativas consideradas	No han podido considerarse otras alternativas al ser imperativa 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.
CONTENIDO Y ANÁLISIS JURÍDICO	
Tipo de norma	Ley
Estructura de la norma	El anteproyecto se estructura en una exposición de motivos, cincuenta artículos distribuidos en siete capítulos, ocho disposiciones adicionales, tres disposiciones transitorias y cinco disposiciones finales.
Informes recabados y pendientes de recabar	El anteproyecto es fruto de un largo proceso de reflexión y estrecha colaboración con los diferentes centros directivos del Ministerio del Interior: Secretaría de Estado de Seguridad (Dirección General de Coordinación y Estudios) y Secretaría General Técnica, que ya ha informado. De conformidad con lo dispuesto en el artículo 26.5, párrafo primero, de la Ley 50/1997, de 27 de noviembre, **se recabará** informe de los siguientes Ministerios: • Ministerio de Defensa. • Ministerio para la Transformación Digital y de la Función Pública. • Ministerio de Transportes y Movilidad Sostenible. • Ministerio de Ciencia, Innovación y Universidades. • Ministerio para la Transición Ecológica y el Reto Demográfico. • Ministerio de Industria y Turismo. • Ministerio de Agricultura, Pesca y Alimentación. • Ministerio de Política Territorial y Memoria Democrática. • Ministerio de Sanidad. • Ministerio de Presidencia del Gobierno (Departamento de Seguridad Nacional). Asimismo, se recaba: • Informe de la Oficina de Coordinación y Calidad Normativa (artículo 26.9 de la Ley 50/1997, de 27 de noviembre) Otros informes o dictámenes: • Agencia Española de Protección de Datos. • Consejo de Estado. **Del mismo modo, se encuentra pendiente de solicitar, conforme al artículo 26.5, párrafo sexto, informe al Ministerio de Política Territorial y Memoria Democrática.**

Trámite de audiencia	Se ha realizado un trámite de consulta pública previa, entre el 21 de septiembre y el 17 de octubre de 2023, previsto en el artículo 133 de la de la Ley 39/2015, de 1 de octubre, y en el artículo 26 de la Ley 50/1997, de 27 de noviembre, en el que se han recibido diversas observaciones. Además, deberá ser sometido al trámite de audiencia e información pública.	
ANÁLISIS DE IMPACTOS		
ADECUACIÓN AL ORDEN DE COMPETENCIAS	Se dicta al amparo de lo establecido en el artículo 149.1. 29ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de seguridad pública. Se respeta, por tanto, el orden constitucional de distribución de competencias.	
IMPACTO ECONÓMICO Y PRESUPUESTARIO	**Efectos sobre la economía en general.**	Tiene un impacto económico positivo sobre el sector económico al que se imponen obligaciones.
	En relación con la competencia	☒ La norma no tiene efectos significativos sobre la competencia. ☐ La norma tiene efectos positivos sobre la competencia. ☐ La norma tiene efectos negativos sobre la competencia.
	Desde el punto de vista de las cargas administrativas	☐ Supone una reducción de cargas administrativas. Cuantificación estimada: ☒ Incorpora nuevas cargas administrativas. Cuantificación estimada: ☐ No afecta a las cargas administrativas.
	Desde el punto de vista de los presupuestos, la norma ☐ Afecta a los presupuestos de la Administración del Estado. ☐ Afecta a los presupuestos de otras Administraciones Territoriales.	☒ Implica un gasto. ☐ Implica un ingreso.

IMPACTO DE GÉNERO	La norma tiene un impacto de género	☐ Negativo ☒ Nulo ☐ Positivo
IMPACTO EN MATERIA DE INFANCIA, ADOLESCENCIA Y FAMILIA	La norma tiene un impacto en la infancia, adolescencia y familia:	☐ Negativo ☒ Nulo ☐ Positivo
IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES	La norma tiene un impacto en la protección de datos personales:	☐ Negativo ☐ Nulo ☒ Positivo
OTROS IMPACTOS CONSIDERADOS	No existen otros impactos significativos.	
EVALUACIÓN "EX POST"	No procede	

2.- OPORTUNIDAD DE LA PROPUESTA.

2.1 Motivación.

Desde la entrada en vigor de la Directiva (UE) 2016/1148 se han logrado considerables progresos en el incremento del nivel de ciberresiliencia de la Unión. La revisión de dicha Directiva ha demostrado que ha servido de catalizador del enfoque institucional y normativo relativo a la ciberseguridad en la Unión, preparando el camino para un cambio significativo de mentalidad. Con ella se ha logrado la realización de marcos nacionales de ciberseguridad mediante la definición de estrategias nacionales de seguridad de las redes y los sistemas de información, el establecimiento de capacidades nacionales y la aplicación de medidas reguladoras que abarcan a las entidades y las infraestructuras esenciales determinadas por cada Estado miembro. Asimismo, la Directiva (UE) 2016/1148 ha propiciado la cooperación a nivel de la Unión mediante el establecimiento del Grupo de Cooperación y de la red de equipos de respuesta a incidentes de seguridad informática. A pesar de estos logros, la revisión de la Directiva (UE) 2016/1148 ha puesto de manifiesto algunas deficiencias inherentes que impiden abordar eficazmente los retos actuales y emergentes en el ámbito de la ciberseguridad.

La seguridad de las redes y los sistemas de información se ha convertido en un aspecto crucial del día a día gracias a la velocidad de la transformación digital y la interconexión de la sociedad y también en los intercambios transfronterizos. Esta evolución ha causado una expansión del panorama de las ciberamenazas, con la consiguiente aparición de nuevos desafíos que requieren respuestas adaptadas, coordinadas e innovadoras en todos los Estados miembros. El número, la magnitud, la sofisticación, la frecuencia y los efectos de los incidentes están en aumento y representan una grave amenaza para el funcionamiento de los sistemas de seguridad en las redes y la información. Como consecuencia de ello, los incidentes pueden interrumpir las actividades económicas en el mercado interior, generar pérdidas financieras, mermar la confianza de los usuarios y ocasionar grandes daños a la economía y la sociedad de la Unión. Por consiguiente, la preparación y la eficacia en materia de ciberseguridad son más esenciales que nunca para que el mercado interior funcione correctamente. Además, la ciberseguridad es un factor facilitador esencial para que muchos sectores críticos se sumen con éxito a la transformación digital y aprovechen plenamente las ventajas económicas, sociales y sostenibles de la digitalización.

Los requisitos impuestos por un Estado miembro que difieren de los aplicados por otro Estado miembro, o incluso los contradicen, pueden afectar sustancialmente a esas actividades transfronterizas. Además, es probable que una concepción o aplicación inadecuadas de los requisitos de ciberseguridad en un Estado miembro tenga repercusiones para el nivel de ciberseguridad de otros Estados miembros, máxime si se tiene en cuenta la intensidad de los intercambios transfronterizos. La revisión de la Directiva (UE) 2016/1148 ha puesto de manifiesto la existencia de grandes diferencias en su aplicación por parte de los Estados miembros, en particular por lo que respecta a su ámbito de aplicación, cuya delimitación se dejó en gran medida a discreción de los Estados miembros. Asimismo, la Directiva (UE) 2016/1148 confería a los Estados miembros una discrecionalidad muy amplia en lo tocante a la aplicación de las obligaciones de seguridad y notificación de incidentes que en ella se establecían. En consecuencia, dichas obligaciones venían aplicándose de manera considerablemente diferente en cada Estado miembro. También existen diferencias similares en la aplicación de las disposiciones de la Directiva (UE) 2016/1148 sobre supervisión y observancia.

Todas esas diferencias conllevan una fragmentación del mercado interior y pueden tener efectos perjudiciales para su funcionamiento, afectando, en particular, a la prestación transfronteriza de servicios y al nivel de ciberresiliencia debido a la aplicación de medidas dispares. En última instancia, esas diferencias podrían derivar en una mayor vulnerabilidad de algunos Estados miembros frente a las ciberamenazas, cuyos efectos podrían sentirse en toda la Unión. El objetivo de la presente Directiva es eliminar estas divergencias tan pronunciadas entre los Estados miembros, concretamente mediante la definición de normas mínimas relativas al funcionamiento de un marco regulador coordinado, el establecimiento de mecanismos para que las autoridades competentes de cada Estado miembro cooperen de manera eficaz, la actualización de la lista de sectores y actividades sujetos a las obligaciones de ciberseguridad y la disponibilidad de vías de recurso y medidas de ejecución eficaces que son fundamentales para garantizar el cumplimiento efectivo de dichas obligaciones. Por consiguiente, procede derogar la Directiva (UE) 2016/1148 y sustituirla por la presente Directiva.

Dada la intensificación y la mayor sofisticación de las ciberamenazas, los Estados miembros deben esforzarse por garantizar que las entidades excluidas del ámbito de aplicación de la presente Directiva alcancen un elevado nivel de ciberseguridad y apoyar la aplicación de medidas equivalentes de gestión de riesgos de ciberseguridad que reflejen el carácter sensible de dichas entidades.

Con estos objetivos, se publicó 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 (Directiva NIS2), 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, objeto de transposición. En ella, se establece como fecha límite para su transposición por los Estados miembros a su ordenamiento jurídico nacional el **17 de octubre de 2024.**

Por parte del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación se designó responsable de la transposición al Ministerio del Interior y

a Presidencia de Gobierno, Ministerio de Defensa, y Ministerio para la Transformación Digital competentes.

2.2. Fines y objetivos que se persiguen.

El principal objetivo perseguido es dar cumplimiento a lo dispuesto en la Directiva que se transpone, y más concretamente:

El anteproyecto de Ley de coordinación y gobernanza de la ciberseguridad transpone 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 (Directiva NIS2), 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 y el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. La Directiva NIS2 busca superar ciertas deficiencias de la Directiva NIS1 recogiendo un marco más completo de obligaciones tanto técnicas como normativas en aras a reforzar la seguridad de las redes y de la información en la Unión Europea.

Este anteproyecto de Ley destaca como su aspecto más novedoso, y uno de los más significativos, la creación de un Departamento 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, asumiendo la función de 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.

También se establece un criterio uniforme para determinar las entidades que están incluidas en el ámbito de aplicación de la presente norma, a efectos del cumplimiento de las medidas para la gestión de riesgos de ciberseguridad, que 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 y volumen de negocio.

Se refuerzan los requisitos de seguridad con una lista de medidas específicas, entre ellas la respuesta a incidentes y la gestión de crisis, el tratamiento y la divulgación de vulnerabilidades, las pruebas de ciberseguridad y el uso eficaz del cifrado. En cuanto a 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 singulares a llevar a cabo por éstas para garantizar y elevar sus niveles de seguridad de los sistemas de redes y 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. En este mismo sentido, se introducen mecanismos de coordinación con la norma por la que se transpone la Directiva 2023/2557 sobre resiliencia de las entidades críticas, cuya transposición también asume este Departamento.

La notificación de incidentes que ya aparecía en NIS 1, se refuerza notablemente, con un procedimiento detallado y exhaustivo de notificación de incidentes al objeto de que se realicen dentro de un marco común de la Unión Europea. Se incluyen disposiciones más precisas sobre el proceso de notificación, el contenido y los plazos, y para dar cumplimiento a las obligaciones de notificación se utilizará la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, que permitirá el intercambio de información técnica y el seguimiento de incidentes entre los distintos actores.

Asimismo, se recoge la figura del responsable de 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. En este contexto, destaca la consideración de la figura del responsable de seguridad de la información de las entidades esenciales a través de la reforma de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

Por último, se establece un régimen sancionador detallado que incluye sanciones efectivas, proporcionales y disuasorias teniendo en cuenta las circunstancias concretas del caso. Las sanciones recogidas pueden llegar para las entidades esenciales hasta los 10.000.000€ o de un máximo de un 2% del volumen de negocio anual total a nivel mundial del ejercicio financiero anterior. Además de las sanciones económicas, también se contempla la posibilidad de otras medidas correctivas, como la supervisión continua, auditorías de seguridad y la imposición de medidas específicas para abordar las deficiencias identificadas en los sistemas de ciberseguridad.

2.3. Adecuación a los principios de buena regulación.

Se analiza a continuación la adecuación de la norma a los principios de buena regulación del artículo 129 de la Ley 39/2015, de 1 de octubre de Procedimiento Administrativo Común de las Administraciones Públicas.

Por un lado, se trata de una norma necesaria para la transposición de la Directiva NIS 2, cuyo artículo 41 dispone que los Estados miembros adoptarán y publicarán a más tardar el 17 de octubre de 2024 las disposiciones necesarias para dar cumplimiento a lo establecido en la presente Directiva.

Es una norma eficaz para la consecución de los objetivos que persigue, esto es:

- Crear una Autoridad Nacional Competente única en materia de ciberseguridad con funciones de dirección y coordinación.
- Designación de las Autoridades de Control, con funciones ejecutivas.
- Definir un criterio uniforme para determinar las entidades que están incluidas en el ámbito de aplicación clasificadas en entidades esenciales y entidades importantes.
- Establecer un catálogo de medidas necesarias para la gestión de riesgos de ciberseguridad.
- Reforzar el procedimiento de notificación de incidentes que perturben o puedan perturbar la prestación de los servicios de entidades esenciales e importantes.
- Crear la figura del responsable de seguridad de la información.

- Reforzar las normas y obligaciones relativas al intercambio de información sobre ciberseguridad.
- Establecer un marco institucional y de coordinación entre las autoridades competentes.

Respecto al principio de seguridad jurídica, se trata de una norma con rango de ley, cuya tramitación e integración en el ordenamiento jurídico goza de las garantías que amparan a las normas de este rango.

Este anteproyecto es coherente también con el principio de proporcionalidad exigible en el desarrollo de cualquier derecho. Contempla una gran cantidad de 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.

Por último, cumple también con el principio de transparencia exigible, habiendo sido sometida ya al trámite de consulta pública previa para someterse después al resto de trámites que garantizan la participación pública.

2.4. Alternativas.

La Directiva objeto de transposición contiene regulación sobre seguridad de las redes y sistemas de información a través de un modelo de coordinación y gobernanza de la ciberseguridad. Dicha Directiva exige en su artículo 41 a los Estados miembros la adopción de las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo dispuesto en la misma estableciendo un plazo para ello.

Esta ley tiene por objeto la adaptación a nuestro ordenamiento jurídico 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.

Además, el anteproyecto tiene una regulación muy pormenorizada sobre el Departamento Nacional de Ciberseguridad, que actuará como punto de contacto único para garantizar la cooperación intersectorial con las autoridades de control y puntos de contacto sectoriales a nivel nacional, así como una labor de enlace que garantice la cooperación transfronteriza con las autoridades competentes en otros estados miembros y la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

Por todo ello, descartada esta posibilidad, la única alternativa posible es la aprobación de una ley que incorpore al ordenamiento jurídico español lo previsto en dicha Directiva.

Respecto al rango de la ley, teniendo en cuenta que se trata de una norma que no afecta a derechos fundamentales, la transposición no exige la aprobación de una ley con rango de orgánica, tal y como viene exigido por el artículo 81.1 de la Constitución española.

3.- CONTENIDO, ANÁLISIS JURIDICO Y DESCRIPCIÓN DE LA TRAMITACIÓN.

I. Contenido.

El anteproyecto se divide en cuarenta y nueve artículos, estructurados en siete capítulos, así como de ocho disposiciones adicionales, tres disposiciones transitorias, una disposición derogatoria y cuatro disposiciones finales, que incluyen tanto aquellos aspectos de obligado desarrollo por venir así dispuesto en la Directiva NIS2, como aquellos otros que, sin previsión específica, se ha considerado oportuno abordar, toda vez que ofrecen oportunidades y ventajas en las actuaciones de protección de la ciberseguridad.

- **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.

En este sentido, se establece como objeto alcanzar un elevado nivel común de ciberseguridad a través de la adopción de una estrategia nacional de ciberseguridad y la designación o establecimiento de autoridades competentes, 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); junto a un catálogo de medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades reguladas en esta ley; normas y obligaciones relativas al intercambio de información sobre ciberseguridad y obligaciones de supervisión y ejecución.

La ley se aplica a las entidades públicas o privadas que se encuentren dentro de los sectores de alta criticidad y otros sectores críticos recogidos en los Anexos I y II de la misma, cuando sean consideradas medianas o grandes empresas al ocupar a 50 o más personas y cuyo volumen de negocios anual o cuyo balance general anual alcance o supere los 10 millones de euros. Asimismo, es de aplicación Independientemente de su tamaño, a las entidades comprendidas en los tipos señalados en los Anexos I o II de la Ley, cuando:

a) Los servicios prestados lo sean por proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público, prestadores de servicios de confianza y registros de nombres de dominio 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 pública, el orden público o la salud pública.

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 sea una entidad del sector público, tal y como se encuentra definido en el artículo 2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
f) Aquellas 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 con el 25 % o más de su capital o de sus derechos de voto controlados, directa o indirectamente, por uno o más organismos públicos, y que sean así identificadas por la autoridad competente, salvo que pueda ser considerada una empresa vinculada.
i) Cualquier otra entidad que la autoridad competente correspondiente identifique como entidad esencial aplicando los criterios del presente artículo, mediante resolución motivada.

- **Capítulo II.**

El capítulo II establece el marco nacional, estratégico e institucional, para la seguridad de las redes y sistemas de información, con el 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 Cibserseguridad, destacando, entre otros, la definición de los objetivos y sus prioridades, particularmente en lo referido a los sectores mencionados en los anexos I y II de la ley, la relación de las autoridades y partes interesadas que participan en la ejecución de la Estrategia Nacional de Ciberseguridad, un marco de gobernanza para lograr los objetivos y prioridades definidos en la estrategia de ciberseguridad, un marco de gobernanza que aclare las funciones y responsabilidades de las partes interesadas, y que sustente la cooperación y la coordinación entre las mismas a nivel nacional, un mecanismo para la identificación de los activos pertinentes, la evaluación de los riesgos de ciberseguridad, la determinación de las medidas para garantizar la preparación, la capacidad de respuesta y la recuperación frente a incidentes, incluida la cooperación entre los

sectores público y privado y plan de medidas necesarias para elevar el nivel general de concienciación de los ciudadanos en materia de ciberseguridad.

A destacar como la principal novedad y el aspecto más significativo de este capítulo, se contempla la existencia de un Departamento Nacional de Ciberseguridad, que, superando la actual dispersión competencial en materia de ciberseguridad, se constituye en autoridad nacional competente única en la materia para el 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 sectoriales, así como autoridad nacional de gestión de crisis de ciberseguridad y equipo de respuesta a incidentes de ciberseguridad nacional de referencia.

Además, se especifican las funciones que debe ejercer el Departamento Nacional de Ciberseguridad, entre las que destacan, funciones de dirección y supervisión tales como promover y aprobar, en su caso, el uso de estándares, guías, especificaciones, instrucciones técnicas y cualquier disposición en materia de seguridad de las redes y sistemas de información, e 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.

Igualmente, se detallan las funciones de las Autoridades de control, quienes serán, en el marco de sus competencias, las encargadas de las funciones de supervisión y ejecución tales como: establecer canales de comunicación con las entidades esenciales e importantes, entre los que se incluyen la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, 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, informar al público sobre determinados incidentes, participar, de forma voluntaria, en las revisiones interpares o proponer las medidas de gestión de riesgos de ciberseguridad de obligado cumplimiento para las entidades incluidas en el ámbito de aplicación de esta norma.

Las Autoridades de control serán:

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.

Además, se contempla la existencia de Puntos de contacto especializados, encargados, entre otras cosas de aportar al Departamento Nacional de Ciberseguridad la información necesaria para la elaboración de estándares de cumplimiento que puedan tener en cuenta las posibles especificidades de cada sector.

En cuanto a los Equipos de respuesta a incidentes de ciberseguridad (CSIRT) nacional de referencia, se concreta que, en materia de seguridad de las redes y sistemas de información, son 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.

2º El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, al que corresponde la comunidad de referencia constituida por las entidades consideradas 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 del Ministerio de Defensa y 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.

Si bien, 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 juntamente con el CSIRT de referencia correspondiente.

- **Capítulo III.**

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 singulares a llevar a cabo por éstas para garantizar y elevar sus niveles de seguridad de los sistemas de redes y de información y prevenir el riesgo de incidentes en el marco del Esquema Nacional de Seguridad y las normas técnicas europeas e internacionales equivalentes.
Por otro lado, se establece a las entidades 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.

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 el Departamento Nacional de Ciberseguridad y con Los CSIRT nacionales de referencia. Esta persona responsable de la seguridad de la información actuará como punto de contacto con el Departamento Nacional de Ciberseguridad en materia de supervisión de los requisitos de seguridad de las redes y sistemas de información y como punto de contacto especializado para la coordinación de la gestión de los incidentes con Los CSIRT nacionales de referencia.

En cuanto a la notificación de incidentes, se toma en consideración el crecimiento de la magnitud, sofisticación, de los incidentes, así como el hecho de que representan una grave amenaza para el funcionamiento de los sistemas de

redes y de información, pudiendo interrumpir las actividades económicas en el mercado interior, y generar grandes pérdidas financieras, lo que puede contribuir a mermar la confianza de los usuarios y ocasionar grandes daños a la economía y la sociedad de la Unión.

Dado lo anterior, se apuesta por un enfoque en varias etapas respecto a la notificación de incidentes significativos para alcanzar un equilibrio entre, por un lado, una notificación ágil que reduzca la posible propagación de incidentes significativos, y, por el otro, una notificación minuciosa que extraiga lecciones valiosas de cada incidente en aras a mejorar la ciberresiliencia de las entidades individualmente y de sectores completos.

Además, la nueva norma aboga por el establecimiento de canales únicos que faciliten la comunicación de los ciberincidentes, lo que impulsa la implementación de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, que ya había sido recogida en la normativa anterior, pero está en vías de concreción.

Por consiguiente, la preparación y la eficacia en materia de ciberinicidentes son más esenciales que nunca para que el mercado interior funcione correctamente.

- **Capítulo IV.**

Por su parte, lo más destacado del capítulo IV consiste en la imposición de la obligación de la elaboración y actualización periódica de una lista de los proveedores de servicios de infraestructuras digitales de naturaleza transfronteriza.

El Departamento Nacional de Ciberseguridad elaborará y mantendrá un registro que contenga la lista de este tipo de entidades. 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 una información determinada, así como cualquier cambio que se produzca en la misma en el plazo de 3 meses desde la fecha en que se produjo el cambio.

- **Capítulo V.**

Al mismo tiempo, el capítulo V consagra el 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 al CSIRT nacional de referencia de aquellos incidentes para los que no se establezca una obligación de notificación.

- **Capítulo VI.**

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

- **Capítulo VII.**

En este capítulo se contempla el régimen sancionador. Se regula la responsabilidad disciplinaria; la competencia sancionadora; los criterios de graduación de las sanciones; la tipificación de las infracciones, clasificadas estas en muy graves, graves y leves; las sanciones aplicables a cada clase de infracciones; las consecuencias de la comisión de las infracciones por las Administraciones Públicas; la prescripción de las infracciones y sanciones; y el procedimiento sancionador.

- **Disposiciones adicionales**

- Primera
  - Se dedica a la creación del Departamento Nacional de Ciberseguridad como autoridad nacional competente única en materia de ciberseguridad.
- Segunda
  - Contiene el Régimen aplicable al Banco de España, al Banco Central Europeo y al Sistema Europeo de Bancos Centrales, de conformidad con la legislación vigente.

- Tercera
    - Establece que 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.
- Cuarta
    - En relación con la Plataforma nacional de Notificación y Seguimiento de Ciberincidentes remite a 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.
- Quinta
    - Aborda la base de datos de incidencias de seguridad que revistan carácter delictivo, atribuyendo la responsabilidad del tratamiento de esta base de datos a la Dirección General de Coordinación y Estudios de la Secretaría de Estado de Seguridad
- Sexta
    - Establece la salvaguarda de intereses y funciones estatales esenciales, de manera que, las obligaciones de la ley 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
- Séptima
    - Establece que, la Secretaría de Estado de Digitalización e Inteligencia Artificial 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.
- Octava
    - Designa a la Autoridad Nacional de Certificación de la Ciberseguridad.

o Disposiciones transitorias

- Primera: Regula las obligaciones de comunicación.
- Segunda: Aborda el registro de entidades. 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 referidas en la ley.
- Tercera: Regula el régimen transitorio

o Disposición derogatoria

Se deroga el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, así como el 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. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta ley

o Disposiciones finales

- Primera: Relativa al título competencial.
- Segunda: Modifica el apartado 9 del artículo 2 y apartado 2 del artículo 3 de la Ley 5/2014, de 4 de abril, de Seguridad Privada.
- Tercera: Se habilita a determinados departamentos ministeriales al desarrollo reglamentario de la norma.
- Cuarta: Mediante la que se incorpora al Derecho español la Directiva NIS2.
- Quinta: A través de la cual se prevé la entrada en vigor de la norma.

2. Análisis jurídico.

2.1. Tabla de correspondencia.

A continuación, se recoge una tabla de correspondencia entre los preceptos de la Directiva NIS2 y los del anteproyecto de ley orgánica.

DIRECTIVA NIS2	ANTEPROYECTO DE LEY
Artículo 1. Objeto.	**Artículo 1.** Objeto.

Artículo 2. Ámbito de aplicación.	**Artículo 3.** Ámbito de aplicación.
Artículo 3. Entidades esenciales e importantes.	**Artículo 4.** Entidades esenciales e importantes.
Artículo 4. Actos jurídicos sectoriales de la Unión.	
Artículo 5. Armonización mínima.	**Disposición adicional sexta.** Salvaguarda de intereses y funciones estatales esenciales
Artículo 6. Definiciones.	**Artículo 2**. Definiciones
Artículo 7. Estrategia nacional de ciberseguridad.	**Artículo 5.** Estrategia nacional de ciberseguridad.
Artículo 8. Autoridades competentes y puntos de contacto únicos.	**Artículo 6.** Autoridad competente. **Artículo 7.** Punto de contacto único.
Artículo 9. Marcos nacionales de gestión de crisis de ciberseguridad.	**Artículo 8.** Marco nacional de gestión de crisis de ciberseguridad.
Artículo 10. Equipos de respuesta a incidentes de seguridad informática (CSIRT).	**Artículo 9**. Equipo de respuesta a incidentes de ciberseguridad (CSIRT) nacional de referencia
Artículo 11. Obligaciones, capacidades técnicas y cometidos de los CSIRT.	**Artículo 10.** Obligaciones, capacidades técnicas y cometidos de los CSIRT nacionales de referencia
Artículo 12. Divulgación coordinada de las vulnerabilidades y una base de datos europea de vulnerabilidades.	**Artículo 11.** Divulgación coordinada de las vulnerabilidades
Artículo 13. Cooperación a escala nacional.	**Artículo 12.** Cooperación a escala nacional
Artículo 14. Grupo de Cooperación.	**Artículo 13.** Cooperación en el ámbito de la Unión Europea
Artículo 15. Red de CSIRT.	**Artículo 13.3.** Cooperación en el ámbito de la Unión Europea
Artículo 16. Red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe).	**Artículo 13.2.** Cooperación en el ámbito de la Unión Europea
Artículo 17. Cooperación internacional.	**Artículo 13.** Cooperación en el ámbito de la Unión Europea
Artículo 18. Informe sobre la situación de la ciberseguridad en la Unión.	
Artículo 19. Revisiones interpares.	**Artículo 13.4.** Cooperación en el ámbito de la Unión Europea
Artículo 20. Gobernanza	**Artículo 14.** Gobernanza
Artículo 21. Medidas para la gestión de riesgos de ciberseguridad	**Artículo 15.** Medidas generales para la gestión de riesgos de ciberseguridad
Artículo 22. Evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas a escala de la Unión	**Artículo 15.3.** Medidas generales para la gestión de riesgos de ciberseguridad.
Artículo 23. Obligaciones de notificación	**Artículo 18.** Obligaciones de notificación.

Artículo 24. Utilización de esquemas europeos de certificación de la ciberseguridad	**Artículo 33**. Utilización de esquemas europeos de certificación de la ciberseguridad
Artículo 25. Normalización	
Artículo 26. Jurisdicción y territorialidad	**Artículo 3.** Ámbito de aplicación
Artículo 27. Registro de entidades	**Artículo 26.** Registro de entidades
Artículo 28. Base de datos sobre el registro de nombres de dominio	**Artículo 27.** Base de datos sobre el registro de nombres de dominio
Artículo 29. Mecanismos de intercambio de información sobre ciberseguridad	**Artículo 28.** Mecanismos de intercambio de información sobre ciberseguridad
Artículo 30. Notificación voluntaria de información pertinente	**Artículo 29.** Notificación voluntaria de información pertinente
Artículo 31. Aspectos generales relativos a la supervisión y la ejecución	**Artículo 30.** Aspectos generales relativos a la supervisión de entidades esenciales e importantes
Artículo 32. Medidas de supervisión y ejecución relativas a entidades esenciales	**Artículo 31.** Medidas de supervisión y ejecución relativas a entidades esenciales
Artículo 33. Medidas de supervisión y ejecución en relación con entidades importantes	**Artículo 32.** Medidas de supervisión y ejecución en relación con entidades importantes
Artículo 34. Condiciones generales para la imposición de multas administrativas a entidades esenciales e importantes	**Artículo 35y siguientes.** Potestad sancionadora
Artículo 35. Incumplimientos que conllevan una violación de la seguridad de los datos personales	**Artículo 24.** Cooperación en lo relativo a los incidentes que afecten a datos personales
Artículo 36. Sanciones	**Artículo 40.** Sanciones.
Artículo 37. Asistencia mutua	**Artículo 34.** Cooperación transfronteriza

2.2. Obligaciones periódicas contenidas en la Directiva.

La Directiva establece una serie de plazos y fechas límite que todos los Estados miembros han de respetar tanto para la transposición de la misma a sus respectivas legislaciones internas como para la elaboración y remisión de informes estadísticos anuales que servirán como base a la Comisión para informar al Parlamento y al Consejo.

El artículo 41 señala como fecha tope para la transposición de la Directiva el 17 de octubre o de 2024.

El artículo 4 de la Directiva establece que, a más tardar el 17 de abril de 2025, y posteriormente cada dos años, las autoridades competentes notificarán a la Comisión y al Grupo de Cooperación, el número de entidades esenciales e importantes enumeradas respecto de cada sector y subsector a que se refieren los anexos I o II, y el tipo de servicio que prestan.

Asimismo, se establece que los Estados miembros deben comunicar a la Comisión sus estrategias y las actualizaciones sustanciales de estas. La Comisión debe elaborar un informe de síntesis de las estrategias comunicadas por los Estados miembros que sirva de base para los intercambios a fin de determinar las mejores prácticas y las cuestiones de interés común.

El artículo 9 recoge que, en el plazo de tres meses a partir de la designación o el establecimiento de la autoridad de gestión de crisis de ciberseguridad, cada Estado miembro notificará a la Comisión la identidad de su autoridad y cualquier modificación posterior de esta. Los Estados miembros presentarán a la Comisión y a la red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe, por sus siglas en inglés) información pertinente relativa a los requisitos sobre sus planes nacionales de respuesta a incidentes y crisis de ciberseguridad a gran escala en un plazo de tres meses a partir de la adopción de dichos planes. Los Estados miembros podrán excluir la información cuando y en la medida en que sea necesario para su seguridad nacional.

El artículo 10 establece que cada Estado miembro notificará sin dilación indebida a la Comisión la identidad del CSIRT designado coordinador, y sus respectivas tareas desempeñadas en relación con las entidades esenciales e importantes.

El artículo 16 establece que a más tardar el 17 de julio de 2024 y posteriormente cada dieciocho meses, la EU-CyCLONe presentará al Parlamento Europeo y al Consejo un informe de evaluación de su labor.

Estas obligaciones de comunicación se incluyen en la Disposición transitoria primera. En concreto, el Consejo Nacional de Ciberseguridad, a través del Departamento de Seguridad Nacional, notificará, antes del 17 de abril de 2025:

- 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

- 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 Departamento Nacional de Ciberseguridad.

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. Además, 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.

Asimismo, 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.

3. Tramitación.

Se trata de una norma incluida en el Plan Anual Normativo para 2024. El anteproyecto ha sido elaborado después de un largo proceso de reflexión.

En la elaboración del texto han intervenido activamente los diferentes centros directivos del Ministerio del Interior.

Se ha realizado un trámite de consulta pública previa, entre el 21 de septiembre y el 17 de octubre de 2023, previsto en el artículo 133 de la de la Ley 39/2015, de 1 de octubre, y en el artículo 26 de la Ley 50/1997, de 27 de noviembre, en el que se han recibido diversas observaciones de las siguientes entidades: Cámara de Comercio, Confederación Española de Organizaciones Empresariales (CEOE), Digitales, Fundación empresa, seguridad y sociedad; Vodafone, Cotec y Ametic.

Las diferentes entidades consideran positivo avanzar en un marco común en relación con la ciberseguridad de los estados miembros, y aportan observaciones específicas dirigidas a: reforzar la necesidad de establecer estándares de seguridad y sistemas de certificación unificados a escala europea, la aplicación de un enfoque basado en el riesgo priorizando las tareas de supervisión, la implementación de la seguridad de la cadena de suministro basada en hechos y criterios objetivos y no discriminatorios, procedimientos claros y precisos de notificación de incidente y la existencia de una ventanilla única para la notificación de los incidentes. Todas estas cuestiones han sido abordadas en el anteproyecto que se tramita.

De conformidad con lo dispuesto en el artículo 26.5, párrafo primero, de la Ley 50/1997, de 27 de noviembre, **se recabará** informe de los siguientes Ministerios:

- Ministerio de Defensa.
- Ministerio para la Transformación Digital y de la Función Pública.
- Ministerio de Transportes y Movilidad Sostenible.
- Ministerio de Ciencia, Innovación y Universidades.
- Ministerio para la Transición Ecológica y el Reto Demográfico.
- Ministerio de Industria y Turismo.
- Ministerio de Agricultura, Pesca y Alimentación.
- Ministerio de Política Territorial y Memoria Democrática.
- Ministerio de Sanidad.
- Ministerio de Presidencia del Gobierno (Departamento de Seguridad Nacional).

Asimismo, debe recabarse informe de:

- **Ministerio de Política Territorial y Memoria Democrática (artículo 26.5, párrafo sexto, de la Ley 50/1997, de 27 de noviembre)**
- La Oficina de Coordinación y Calidad Normativa (artículo 26.9 de la Ley 50/1997, de 27 de noviembre)
- Agencia Española de Protección de Datos.

Además, deberá recabarse el dictamen preceptivo del Consejo de Estado.

Una vez concluidos estos trámites, el anteproyecto será remitido al consejo de ministros para su aprobación como proyecto de ley y posterior remisión al Congreso de los Diputados.

Esta norma tiene vigencia indefinida y entrará en vigor al mes de su publicación en el "Boletín Oficial del Estado". Con ello, se excepciona la regla general recogida en el artículo 23 de la Ley 50/1997, de 27 de noviembre, según la cual la vigencia de las normas que impongan nuevas obligaciones a las personas físicas o jurídicas que desempeñen una actividad económica o profesional comenzará el 2 de enero o el 1 de julio siguientes a su aprobación. No obstante, el propio apartado segundo del artículo 23 prevé ciertas situaciones en las que no será de aplicación esta regla general, como cuando lo aconseje el cumplimiento del plazo de transposición de una directiva, supuesto que se da en esta ley.

4.- ANÁLISIS DE IMPACTOS.

4.1. Impacto económico y presupuestario.

4.1.1 Efectos en los precios

Las entidades esenciales e importantes deben implementar una serie de medidas técnicas, organizativas y de seguridad adecuadas y proporcionadas para garantizar el cumplimiento de la ley.

En este contexto, las entidades esenciales designarán a una persona, unidad u órgano colegiado como responsable de seguridad, que ejercerá las funciones de punto de contacto y coordinación técnica con el Departamento

Nacional de Ciberseguridad y con Los CSIRT nacionales de referencia. En el supuesto de que el responsable de seguridad sea una unidad u órgano colegiado se deberá designar una persona física representante, así como un sustituto de este que asumirá sus funciones en casos de ausencia, vacante o enfermedad. Las entidades esenciales comunicarán al Departamento Nacional de Ciberseguridad la designación del responsable de seguridad dentro del plazo de tres meses desde la adquisición de la condición de tales. Asimismo, comunicarán los sucesivos nombramientos y ceses que afecten a su nominación en el plazo de un mes desde que aquellos se produzcan.

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 obtener en el marco de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad y la Ley 5/2014, de 4 de abril, de Seguridad Privada y en la forma que reglamentariamente se establezca, la condición de personal acreditado. En el caso de tratarse de entidades esenciales que también tengan la consideración de críticas conforme a la ley XXXXXXX, esta obligación será asimismo extensiva al resto de personal de ciberseguridad.

Las medidas recogidas en la norma buscan mejorar la seguridad de la redes y sistemas de información, la respuesta de las entidades antes ciberataques y como se ha analizado se establece un marco de gobernanza con la política de seguridad de la información como pieza esencial. Asimismo, se refuerzan los requisitos de seguridad con una lista de medidas, entre ellas la respuesta a incidentes y la gestión de crisis, el tratamiento y la divulgación de vulnerabilidades, las pruebas de ciberseguridad y el uso eficaz del cifrado. También se refuerzan las medidas de protección de la cadena de suministro de las principales tecnologías de la información y la comunicación.

En este contexto, el esfuerzo económico dedicado a la implementación de estas medidas de seguridad debe considerarse como una inversión, puesto que genera rendimientos positivos como resultado de la reducción del impacto de los incidentes de seguridad.

4.1.2 Efectos en la productividad.

Las medidas tendrán un efecto positivo sobre la productividad. El incremento de las medidas técnicas, organizativas y de seguridad adecuadas y proporcionadas para garantizar la seguridad junto con la mayor eficacia en la gestión de los riesgos de incidentes de seguridad, reducirá el impacto perjudicial de estos incidentes en los servicios, redundando en una mayor productividad en su prestación.

4.1.3 Efectos en el empleo.

Las medidas tendrán un efecto positivo sobre el empleo, dado que se refuerzan las obligaciones en cuanto a los medios personales dedicados a la seguridad de las redes y sistemas de información.

4.1.4 Efectos sobre la innovación

Estas medidas técnicas, organizativas y de seguridad adecuadas y proporcionadas tendrán un efecto positivo sobre la innovación. Las entidades afectadas deben ser capaces de prevenir los ataques híbridos, las catástrofes naturales, las amenazas terroristas y las emergencias de salud pública y de protegerse, responder, resistir y recuperarse frente a ellos.

4.1.5 Efectos sobre los consumidores

Las medidas tendrán un efecto positivo sobre los consumidores. Los incrementos de productividad e innovación en la prestación de los servicios contribuirán a dinamizar los mercados de los diferentes sectores considerados, con el consiguiente aumento de la demanda de dichos servicios por parte de los consumidores.

4.1.6 Efectos en relación con la economía europea y otras economías.

Las medidas tendrán un efecto positivo en relación con la economía europea. Dado que el proyecto desarrolla la norma nacional de 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, cuyo objetivo es adaptarse a la rápida evolución del panorama de amenazas, con la adopción de medidas de mejora de la seguridad de las redes y

sistemas de información de las entidades esenciales e importantes en el ámbito de aplicación de la norma.

4.1.7 Efectos en la competencia y la unidad de mercado.

El proyecto tiene un efecto neutral en la competencia en los diferentes mercados afectados y se adecúa a lo dispuesto en la Ley 20/2013, de 9 de diciembre, de Garantía de la Unidad de Mercado. Por otra parte, las obligaciones para las entidades críticas se definen de acuerdo con el principio de proporcionalidad, afectando por igual a todos los operadores de cada sector que cumplan determinados criterios, correspondiendo a las autoridades sectoriales la concreción de dichos criterios en el ámbito de que se trate.

4.1.8 Impacto presupuestario.

A) Desde el punto de vista del gasto.

- **Impacto en las entidades (Anexo 1)**

Para la valoración del impacto económico que produce en las empresas la trasposición de la Directiva NIS 2 se ha llevado a cabo un complejo proceso que se detalla a continuación. En primer lugar, se ha realizado una estimación del número de entidades obligadas por la norma según los datos recogidos en el Instituto Nacional de Estadística, junto a los informes recabados por la Secretaría de Estado de Seguridad en el ejercicio de sus funciones de autoridad competente en virtud del RDL 12/2018, en base a la categorización de entidades por el número de empleados.

Si bien, dentro de las entidades esenciales se ha distinguido entre aquellas que se encontraban bajo el ámbito de aplicación de la NIS1 (300) y las que no (1519), como resultado de este proceso se han identificado un total de 1.819 entidades esenciales, y 3.941 entidades importantes.

A continuación, se ha realizado una estimación del coste medio que tendría para cada entidad la asunción de obligaciones que se derivan de la trasposición de la directiva NIS 2, siendo éste de 179.562,50 € para las entidades importantes, y de 2.153.250,00 € para las esenciales.

Ahora bien, teniendo en cuenta que la Directiva NIS 1 traspuesta a nuestro ordenamiento jurídico a través del RD 43/2021 y derogada por la NIS 2, ya imponía a determinadas empresas ciertas obligaciones en materia de ciberseguridad, que éstas venían cumpliendo, el punto de partida para la puesta en marcha de la NIS 2 no sería de cero, por lo que se ha realizado una labor de estimación de este concepto con la intención de aplicarlo como índice corrector en el cálculo del coste total.

En este sentido, se han identificado los siguientes porcentajes medios de implantación previa de requisitos exigidos por la NIS2 en función del tipo de entidad:

- Entidades importantes: 27%
- Entidades esenciales no reguladas previamente por NIS1: 48%
- Entidades esenciales sí reguladas previamente por NIS1: 95%

De manera que, una vez aplicados estos porcentajes al coste medio por entidad se obtienen los importes reflejados en la columna de coste medio corregido por entidad.

Con todo lo expuesto anteriormente, y como resultado de aplicar los índices correctores mostrados en la tabla al coste medio, se han obtenido las cifras que aparecen sombreadas en tono gris en la última columna, lo que supone un total de 2.249.696.603,13 €, que sería, de forma aproximada, el coste total para la plena implantación de la norma en el tejido empresarial español.

TIPO DE ENTIDAD	NÚMERO APROXIMADO DE ENTIDADES	COSTE MEDIO/ENTIDAD	%IMPLANTACIÓN PREVIA MEDIA REQUISITOS	COSTE MEDIO CORREGIDO/ENTIDAD	COSTE TOTAL CORREGIDO
IMPORTANTES	3941	179.562,50 €	27	131.080,63 €	516.588.743,13 €
ESENCIALES NO REGULADAS PREVIAMENTE NIS1	1519	2.153.250,00 €	48	1.119.690,00 €	1.700.809.110,00 €
ESENCIALES SÍ REGULADAS PREVIAMENTE NIS1	300	2.153.250,00 €	95	107.662,50 €	32.298.750,00 €
				COSTE TOTAL IMPLANTACIÓN	**2.249.696.603,13 €**

- **Impacto en la Administración**
    - Creación del Departamento Nacional de Ciberseguridad. (Anexo 2)

Con la aprobación del anteproyecto de ley que transpone al ordenamiento jurídico español la Directiva (UE) 2022/2555 de 14 de diciembre de 2022 (Directiva NIS2), relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, se prevé la creación de un departamento Nacional de Ciberseguridad, cuyo impacto económico es el que se refleja a continuación:

B) Desde el punto de vista de los ingresos.

Las medidas adoptadas supondrán ingresos adicionales para el Estado, correspondientes a las habilitaciones de los responsables de seguridad como personal de seguridad privada que se calculan en el apartado de cargas administrativas.

4.1.9 Análisis de las cargas administrativas.

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 obtener en el marco de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad y la Ley 5/2014, de 4 de abril, de Seguridad Privada y en la forma que reglamentariamente se establezca, la condición de personal acreditado. En el caso de tratarse de entidades esenciales que también tengan la consideración de críticas conforme a la ley XXXXXXX, esta obligación será asimismo extensiva al resto de personal de ciberseguridad.

Dado lo anterior, se generará un coste correspondiente a la habilitación del responsable de seguridad de la información como personal de seguridad privada, por lo que se estiman las cargas aplicables enumeradas a continuación.

Se realiza el cálculo de la cantidad tomando el modelo aplicable por la Dirección General de la Policía para los directores y jefes de seguridad.

- Empresas de seguridad privada tasas aplicables a los trámites y procedimientos relacionados con Seguridad Privada.
    - Habilitación operadores de ciberseguridad y los directores de ciberseguridad: 97,23 €.

- Trámites y procedimientos
    - Compulsa de documentos: 3,92 €
    - Incremento por cada página del documento a compulsa: 1,95 €
    - Expedición de certificaciones 23,34 €
    - Incremento por cada página de extensión que exija la certificación 1,95 €

4.2 Impacto por razón de género

Tiene un impacto de género nulo en cuanto que su contenido no incluye ningún tipo de medida que pueda afectar a la igualdad de oportunidades entre hombres y mujeres.

4.3. Impacto en la infancia y en la adolescencia.

Tiene un impacto nulo en la infancia y la adolescencia, ya que no regula nada relacionado con ese ámbito.

4.4. Impacto en la familia.

Tiene un impacto nulo en la familia, ya que no regula nada relacionado con ese ámbito.

4.5. Impacto en materia de medio ambiente y cambio climático

Respecto del impacto por razón del cambio climático, incorporado en la Ley del Gobierno, por la disposición final 5 de la Ley 7/2021, de 20 de mayo, de cambio climático y transición energética, se estima que el impacto que tendrá el anteproyecto sobre el cambio climático en términos de mitigación y adaptación al mismo, utilización y protección sostenibles de los recursos hídricos y marinos,

economía circular, incluidos la prevención y el reciclado de residuos, prevención y control de la contaminación a la atmósfera, el agua o el suelo, y protección y restauración de la biodiversidad y los ecosistemas, será nulo, cumpliendo el principio de no causar daño significativo alguno.

4.6. Impacto en materia de protección de datos

Este análisis se realiza siguiendo el criterio de la Agencia Española de Protección de Datos (AEPD) impartido en las Jornadas de Calidad Normativa en Protección de Datos llevadas a cabo el 23 de mayo de 2023.

La norma tiene un impacto positivo en la protección de datos personales al regular la materia garantizando la protección de este derecho fundamental, en relación con los tratamientos de datos personales que deriven de la aplicación de misma. En la norma se prevé y se determinan distintos tipos de tratamientos de datos.

Dado el alcance que tiene esta norma y los efectos que produce en otras disposiciones legales, se ha realizado un estudio profundo del impacto que tiene la misma en materia de protección de datos. En este sentido, la profundidad y formalidad del presente análisis es acorde al riesgo y al nivel de injerencia producido por la norma en los derechos y libertades de las personas interesadas, en especial, en el derecho fundamental a la intimidad, recogido en el artículo 18.4 de la Constitución. Del mismo modo, resulta importante señalar que durante la tramitación formal de la disposición se solicitará informe preceptivo de distintos organismos entre los que se incluye a la propia AEPD.

En este contexto, el anteproyecto establece en su propio objeto las finalidades de establecer normas específicas de seguridad de los sistemas de información (lo que redunda en las garantías de los datos personales) y fijar las normas y obligaciones relativas al intercambio de información sobre ciberseguridad.

En las definiciones contenidas en la norma, también se recogen descripciones sobre conceptos que afectan o pueden afectar a datos personales como las de redes y sistemas de información, seguridad de las redes y sistemas de información, ciberseguridad, cuasi-incidente, incidente, registro de nombres de dominio de primer nivel y servicio de centro de datos.

El artículo 4 recoge la obligación de remitir a las autoridades de control una serie de datos, entre los que se encuentran identificadores, por lo que cada una de dichas autoridades deberán crear o incorporar dicha información a los correspondientes tratamientos internos.

Conforme al contenido del artículo 9.6, se prevé que los CSIRT nacionales puedan 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, si bien estas actuaciones se realizarán de conformidad con la legislación de la Unión en materia de protección de datos.

Como previsión relevante en el factor que se está analizando, el artículo 12, establece que el Departamento Nacional de Ciberseguridad, cooperará y colaborará con los órganos con competencias, entre otras, en materia de protección de datos personales.

La Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes dispuesta en el artículo 19, contará con los requisitos específicos que apliquen en materia de protección de datos de carácter personal y garantizará tanto las dimensiones de seguridad de la información y los datos como el principio de transparencia. Generando la obligación de que, cada uno de los gestores y usuarios de esta, de acuerdo con sus respectivas competencias, desarrollen los correspondientes tratamientos de datos.

Resulta muy significativo igualmente el contenido del artículo 24, al establecer las obligaciones de las autoridades de control cuando se produzca un incidente que lleve aparejada la afectación a datos personales.

Del mismo modo, se habilita una previsión legal en el artículo 25 para la cesión de identificadores en los supuestos de notificaciones, gestiones, análisis o resoluciones relacionadas con incidentes que limita la cesión al tratamiento de los datos que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso. Incluyéndose un listado de supuestos en los que esta operación se puede llevar a cabo.

En los artículos 26 y 27 se obliga a la cesión de determinados datos personales para incluirlos en los registros de proveedores de servicios e

infraestructuras digitales y en la base de datos sobre el registro de nombres de dominio.

Como tratamiento específico y singular, en la disposición adicional quinta se establece que la Dirección General de Coordinación y Estudios, de la Secretaría de Estado de Seguridad, será el órgano responsable del tratamiento de la base de datos de incidencias de seguridad que revistan carácter de delito. De manera que, los datos comunicados solo serán objeto de tratamiento para el cumplimiento de los fines previstos en la norma, cuando puedan entenderse presuntamente delictivos.

En este tratamiento de datos de incidencias de seguridad 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.

Los destinatarios de estos datos serán los órganos jurisdiccionales del orden penal, el Ministerio Fiscal y las Fuerzas y Cuerpos de Seguridad, así como otras entidades cuando se prevea legalmente, siendo éstos también responsables del tratamiento de los datos que les hubieran comunicado conforme a las disposiciones de esta ley.

El anteproyecto establece que la base jurídica principal del tratamiento de acuerdo con el objetivo y finalidad de la misma es el cumplimiento de 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.

Por otro lado, 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.

Todo ello garantizando el principio de minimización de datos y de información previa a las personas interesadas sobre las condiciones, derechos y obligaciones del tratamiento, así como a los posibles destinatarios en los términos previstos en la ley.

De acuerdo con la finalidad del tratamiento, se establece la obligación de conservación de los datos recogidos durante el tiempo necesario para el cumplimiento del fin para el cual fueron recogidos en virtud del artículo 8 de la Ley Orgánica 7/2021, de 26 de mayo, y en su caso por el tiempo necesario para

atender a las responsabilidades derivadas de su tratamiento ante los órganos administrativos o jurisdiccionales competentes. Una vez trascurrido dicho periodo de conservación, los datos serán suprimidos de manera que se imposibilite la correlación o identificación de estos con los interesados.

Queda garantizado el ejercicio de derechos para las personas físicas sujetas a la normativa de protección de datos, y serán atendidas las solicitudes de tales derechos por el responsable del tratamiento en los términos establecidos en la Ley Orgánica 7/2021, de 26 de mayo.

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.

La inclusión del contenido de estas disposiciones en el anteproyecto ha sido necesaria teniendo en cuenta la jurisprudencia del Tribunal Constitucional y las recomendaciones de Agencia Española de Protección de Datos.

La norma recoge una limitación de los derechos de las personas interesadas, si bien, cumple con las previsiones del artículo 23 del Reglamento General de Protección de Datos, el artículo 15 de la Directiva 680/2016, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y el artículo 24 de la Ley Orgánica 7/2021, de 26 de mayo al respetar en lo esencial los derechos y libertades fundamentales y ser una medida necesaria y proporcionada en una sociedad democrática para salvaguardar la seguridad del Estado, la seguridad pública y la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención.

En la norma se recogen las previsiones mínimas contenidas en los apartados 2 de los mencionados artículos 23 (RGPD) Y 15 (Directiva)

Del mismo modo, las previsiones de la norma se desarrollan conforme al parecer del Tribunal Constitucional (STC 76/2019, de 22 de mayo, publicada en el BOE núm. 151, de 25 de junio de 2019 y con ECLI:ES:TC:2019:76) al exigir que las disposiciones legales que supongan una injerencia en el derecho fundamental a la protección de los datos personales, especialmente cuando se trate de datos de

categoría especial deben: especificar cuál es el interés público esencial que fundamenta la restricción del derecho y la necesidad de tratar los datos personales; regular pormenorizadamente las injerencias al derecho fundamental estableciendo reglas claras sobre el alcance y contenido de los tratamientos de datos que autoriza; establecer las garantías adecuadas frente a la recopilación de los datos personales que autoriza, sin que pueda diferirse a un momento posterior la regulación legal del tratamiento de datos personales de que se trate, ni remitirse al Reglamento General de Protección de Datos, a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales o cualquiera de las leyes especiales que regulan la protección de este derecho, como es la Ley Orgánica 7/2021, de 26 de mayo.

Por su parte, la Agencia Española de Protección de Datos, (Informes 0074/2020, 0077/2020 y 0041/2022) señala que las leyes que suponen la creación de tratamientos de datos, siendo estos de categoría especial, no pueden remitirse de manera genérica al sometimiento a la normativa de protección de datos, sino que deben incluir previsiones específicas sobre la finalidad, el responsable, la base de legitimación, la motivación legal para los datos de categoría especial, el cumplimiento de los principios de tratamiento, la forma básica de acceso a los datos y los derechos de las personas interesadas y sus garantías de ejercicio.

En resumen, en la norma se incluyen las siguientes previsiones:

Con carácter general, la norma identifica claramente la base de legitimación para los distintos tratamientos y las finalidades a llevar a cabo.

Del mismo modo, para cada operación o tratamiento específico, se han tenido en cuenta los juicios de idoneidad, necesidad y proporcionalidad. Conforme al considerando 4 del RGPD cabe señalar que el tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El proyecto respeta todos los derechos fundamentales, en particular la protección de los datos de carácter personal.

Analizado, con carácter general, el riesgo para los derechos y libertades de los ciudadanos cabe señalar que las obligaciones, deberes y prohibiciones contenidas en la misma que pueden afectar al derecho a la protección de datos es de un nivel adecuado por las previsiones de mitigación contenidas en la misma.

La norma posee coherencia jurídica en el marco regulatorio de protección de datos puesto que sus previsiones se formulan siguiendo el contenido de las que resultan aplicables.

A nivel específico:

- Se ha identificado a los responsables de cada uno de los tratamientos y a otros intervinientes.
- Se describen las operaciones y finalidades de los distintos tratamientos.
- Se pueden identificar claramente las bases de legitimación de los tratamientos.
- Cuando es posible y resulta necesario, se identifican las categorías de interesados.
- Se pueden tratar, pero el objetivo de la norma no es tatar datos de personas vulnerables, en particular niños o que afecten a un gran número de personas.
- Los datos personales tratados son adecuados, pertinentes y limitados a lo necesario.
- Se han comprobado los destinatarios de cada tratamiento y que, para dichas operaciones, se cumple con las condiciones normativas.
- No se realizan transferencias internacionales, en el caso de producirse se deberán adaptar a las condiciones oportunas.
- Dado el nivel de la norma y su finalidad, sí se producen intercambios de datos entre autoridades competentes a nivel de la UE.
- No existen decisiones completamente automatizadas que perjudiquen a las personas interesadas ni se realizan perfiles.
- La norma exige que se adopten las medidas técnicas y organizativas de seguridad de cada tratamiento adecuadas al nivel de riesgo.
- No existen formularios en las mismas.

4.7 Impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad de las personas con discapacidad.

La norma proyectada tiene un impacto nulo en materia de igualdad de oportunidades, no discriminación y accesibilidad de las personas con discapacidad al no contemplar medidas que afecten a esas materias.

5. EVALUACIÓN EX POST.

El presente proyecto normativo no se someterá a evaluación ex post al no concurrir las circunstancias que aconsejan su evaluación ex post, previstas en el artículo 28.2 de la Ley 50/1997, de 27 de noviembre, del Gobierno, y en el artículo 3 del Real Decreto 286/2017, de 24 de marzo, por el que se regulan el Plan Anual Normativo y el Informe de Evaluación Normativa de la Administración general del Estado y se crea la Junta de Planificación y Evaluación Normativa.