

Análisis comparativo de la Directiva NIS2 y el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad en España



Guía práctica para la implementación de la Directiva NIS2 en España

En un contexto marcado por la creciente digitalización e interconexión, la seguridad de las redes y los sistemas de información ha pasado a ser un pilar fundamental para el buen desarrollo de las actividades sociales y económicas en nuestra sociedad. En este escenario, la entrada en vigor de la **Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 (en adelante, "Directiva NIS")**, reveló determinadas deficiencias y desafíos en el ámbito de la ciberseguridad dentro de la Unión Europea (en adelante, "UE"). Estos desafíos se manifestaron principalmente en las marcadas diferencias en los niveles de ciberresiliencia entre los Estados miembros derivadas de la aplicación desigual de medidas de seguridad.

Con el fin de abordar estas discrepancias, el 16 de enero de 2023 entró en vigor la **Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, conocida como "NIS 2"**. Esta directiva establece un marco común destinado a identificar las entidades esenciales e importantes, según el grado de criticidad de los sectores en los que operan, y define requisitos específicos de ciberseguridad, gestión de riesgos y obligaciones de notificación que deben cumplir dichas entidades.

Para garantizar la adecuada implementación de esta normativa, los Estados miembros debían completar su transposición antes del 18 de octubre de 2024. En este contexto, las autoridades españolas han promovido un **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad (en adelante, el "Anteproyecto")**, creando un marco nacional de actuación orientado a mantener un alto nivel de ciberseguridad en las redes y sistemas de información de este tipo de entidades.

A continuación, se presenta un cuadro comparativo de la NIS2 y el Anteproyecto, en el que se analizan aspectos clave como el ámbito de aplicación, las autoridades competentes, las medidas de gestión de riesgos y las obligaciones de notificación. Este análisis tiene el objetivo de facilitar la identificación de las principales diferencias y similitudes entre la directiva y la propuesta española, presentadas de forma clara y concisa:

Aspecto	NIS2 (Directiva Europea)	Anteproyecto de Ley (España)
Ámbito de aplicación	Art. 2: Entidades públicas o privadas de los Anexos I y II ¹ de la NIS2 que sean medianas empresas (menos de 250 empleados y con un volumen de negocios anual inferior a 50 millones de euros o un balance inferior a 43 millones de euros) o que superen dichos umbrales y que operen en la UE. Además, también se aplica a estas entidades si su rol es clave en la sociedad, economía o en sectores específicos, independientemente de su tamaño.	El art. 3 establece que las entidades públicas o privadas con residencia fiscal en España, que pertenezcan a sectores críticos según los Anexos I y II del Anteproyecto, y que sean medianas o grandes empresas (50 o más empleados y un volumen de negocios o balance superior a 10 millones de euros), deben cumplir con la normativa. Los Anexos I y II del Anteproyecto se ajustan al ámbito de aplicación de la NIS2, si bien se incorpora el sector de la industria nuclear y las empresas de seguridad privada, que no están contempladas en la referida directiva.
Autoridades competentes	Arts. 8 a 10: Cada Estado Miembro designará: - una entidad competente encargada de la ciberseguridad y un punto de contacto; - una o varias autoridades responsables de la gestión de incidentes y crisis; y - uno o varios CSIRT (equipos de respuesta a incidentes de seguridad informática)	El art. 6 establece, como autoridad competente en España, el Centro Nacional de Ciberseguridad, adscrito a la Secretaría General de la Presidencia del Gobierno. Este actuará como autoridad nacional de gestión de crisis y punto de contacto único, coordinando las autoridades de control y los CSIRT nacionales, como el CCN, INCIBE-CERT y ESPDEF-CERT. Adicionalmente, el Anteproyecto recoge una nueva figura, el 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.
Medidas de gestión de riesgos	El art. 21 establece que las empresas deben gestionar los riesgos cibernéticos mediante políticas de seguridad, análisis de riesgos, gestión de incidentes, continuidad de actividades, seguridad de la cadena de suministro, y protección en el desarrollo y mantenimiento de sistemas. También deben implementar medidas como ciberhigiene, formación en ciberseguridad, uso de criptografía, control de acceso, autenticación multifactorial, y comunicaciones seguras.	Arts. 14 y 15: Los órganos de dirección de las entidades esenciales e importantes tienen la responsabilidad de implementar las medidas establecidas en el art. 21 de la NIS2 y serán responsables en caso de incumplimiento. El Centro Nacional de Ciberseguridad establecerá las medidas concretas a aplicar. Adicionalmente, el responsable de seguridad será el encargado de supervisar y desarrollar la aplicación de las políticas y su efectividad, supervisar el cumplimiento de la normativa y gestionar los incidentes de ciberseguridad.
Obligaciones de notificación	Art. 23: Requiere que se notifiquen al CSIRT o autoridad competente los incidentes de seguridad cibernética significativos sin demora indebida, y en cualquier caso, dentro de las 24 horas posteriores a su detección, así como una descripción más completa en un plazo de 72 horas. También notificarán a los destinatarios en la mayor brevedad cualquier ciberamenaza significativa que les pueda afectar, así como medidas o soluciones a implementar.	Art. 18: Similar a la NIS2, obliga a notificar incidentes de seguridad a su CSIRT nacional de referencia en un plazo máximo de 24 horas, y proporcionar detalles completos dentro de las siguientes 72 horas. También notificarán a los destinatarios en la mayor brevedad cualquier ciberamenaza significativa que les pueda afectar, así como medidas o soluciones a implementar.

¹ El Anexo I se refiere a sectores de alta criticidad, que incluyen, a modo enunciativo y no limitativo, electricidad, sistemas urbanos de calefacción y refrigeración, crudo, gas, hidrógeno, transporte, banca, infraestructuras de mercados financieros, sector sanitario, agua, infraestructura digital, gestión de servicios TIC. El Anexo II añade otros sectores críticos, como por ejemplo los servicios postales y de mensajería, la gestión de residuos, la fabricación, producción y distribución de sustancias y mezclas químicas, la producción, transformación y distribución de alimentos (al por mayor), la fabricación de productos sanitarios, informáticos y maquinaria, los proveedores de servicios digitales y la investigación.

Otro aspecto relevante de la NIS2 son las medidas de supervisión descritas en su art. 33. Este artículo señala que, cuando haya indicios de que una entidad crítica no cumple con la Directiva NIS2, especialmente en lo relativo a los arts. 21 o 23, los Estados miembros deben asegurar que las medidas de supervisión sean eficaces, proporcionales y disuasorias. Para ello, podrán realizar inspecciones in situ, supervisión remota, auditorías de seguridad, análisis, solicitudes de información, acceso a datos y pruebas sobre el cumplimiento de las políticas de ciberseguridad. Esta cuestión también se contempla en el Anteproyecto español como una posible actuación por parte de la autoridad competente, en este caso, el Centro Nacional de Ciberseguridad.

En cuanto al régimen sancionador, la Directiva NIS2 establece sanciones para las entidades esenciales que pueden alcanzar hasta 10 millones de euros o el 2 % del volumen de negocios anual, en caso de incumplir los artículos 21 o 23. Respecto de las entidades importantes, las sanciones pueden ser de hasta 7 millones de euros o el 1,4 % de su volumen anual de negocios. El Anteproyecto español sigue una línea similar, pero clasifica las sanciones en muy graves, graves y leves. Las infracciones muy graves pueden acarrear multas entre 500.001 euros y 10 millones, mientras que las graves pueden llegar a los 500.000 euros.

Adicionalmente, esta directiva hace una mención a la gestión de brechas de seguridad por parte de este tipo de entidades, indicando que deberán notificar estos incidentes de seguridad a las autoridades competentes en protección de datos (en España, la AEPD). Sin embargo, aclara que, si ya se impone una sanción bajo el Reglamento de Protección de Datos, no se podrá aplicar una multa adicional por el mismo incumplimiento bajo la NIS2, aunque sí se podrán tomar medidas de ejecución. Por su parte, el Anteproyecto español subraya la cooperación estrecha entre las autoridades de control y la AEPD, así como con las autoridades autonómicas, para abordar de manera coordinada los incidentes relacionados con violaciones de la seguridad de datos personales.

Finalmente, y con el objetivo de acelerar la creación de un marco normativo en España y adherirse a la normativa europea, el Gobierno ha decidido tramitar con urgencia el Anteproyecto. Esta normativa será de gran relevancia para las empresas españolas que operan en sectores críticos, ya que deberán implementar las medidas establecidas y cumplir con diversas obligaciones. No obstante, será fundamental revisar el texto una vez entre en vigor para verificar si se han realizado modificaciones o ajustes.

Contacto



Luis Francisco Marimón Prats

Socio I Protección de Datos y Tecnología

lmарimon@marimon-abogados.com

Barcelona



Laura Espinós Ramírez

Abogada I Protección de Datos y Tecnología

lespinos@marimon-abogados.com

Barcelona

Marimón Abogados SLP 2025. Este documento es solo para propósitos informativos generales y no pretende proporcionar asesoramiento legal u otro tipo de asesoramiento profesional.