

## NIS2 y responsabilidad del equipo directivo por incumplimiento: claves para la nueva gobernanza de la ciberseguridad

### Resumen

La Directiva (UE) 2022/2555, de 14 de diciembre de 2022, conocida como NIS2, establece un marco reforzado de ciberseguridad en la Unión Europea, con obligaciones más amplias tanto para las entidades públicas y privadas que prestan servicios esenciales, como para sus órganos de dirección.

En España, el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, aprobado en enero de 2025, pero aún no convertido en ley, avanza en la transposición de la norma europea, introduciendo un sistema de autoevaluación (con obligaciones de notificación y sanciones en caso de incumplimiento), la figura del Responsable de Seguridad de la Información y un régimen sancionador escalonado. Además, prevé que los Directivos puedan responder solidariamente de los incumplimientos de su entidad, pudiendo llegar a hacerlo con su patrimonio personal frente a multas de millones de euros.

El nuevo marco implica una transformación profunda en la forma en que las organizaciones gestionan los riesgos digitales, notifican incidentes y articulan la supervisión de sus políticas de ciberseguridad desde el más alto nivel corporativo.

### 1. Un nuevo marco europeo de ciberseguridad

La Directiva NIS2, aprobada el 14 de diciembre de 2022, sustituye a la Directiva NIS1 y busca armonizar los niveles de ciberseguridad en todos los Estados miembros. Su **transposición debía completarse antes del 17 de octubre de 2024**, aunque varios Estados, entre ellos España, han incurrido en retraso, lo que motivó un dictamen motivado de la Comisión Europea en mayo de 2025.

NIS2 amplía el alcance de la regulación al incluir un mayor número de sectores y tipos de entidades, abarcando tanto los considerados **esenciales** (como, por ejemplo, energía, transporte, salud, banca, espacio o infraestructura digital) como los **importantes** (entre ellos, fabricación, alimentación, servicios postales, gestión de residuos o investigación).

### 2. La transposición en España: novedades y obligaciones

El **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad**, aprobado por el Consejo de Ministros el 14 de enero de 2025, adapta al ordenamiento español las exigencias de NIS2 y articula una serie de novedades relevantes. Sin embargo, hay que remarcar que la tramitación parlamentaria para convertirlo en ley presenta cierto retraso.

En primer lugar, introduce un sistema de **autoevaluación y autorregistro** que obliga a las entidades a determinar si se consideran esenciales o importantes y a comunicarlo a la autoridad competente en el plazo de **tres meses**. Este mecanismo refuerza la corresponsabilidad de las organizaciones en el cumplimiento normativo y se acompaña de sanciones que pueden oscilar entre **10.000 y 500.000 euros**, dependiendo de la gravedad de la infracción.

El texto también crea la figura del **Responsable de Seguridad de la Información**, cuyas funciones incluyen la coordinación de medidas técnicas y organizativas de protección, la gestión de incidentes y la interlocución con las autoridades

# Nota informativa

---

competentes. Junto a ello, se establece un régimen sancionador graduado inspirado en la Directiva, con multas que, en los casos más graves, pueden alcanzar los **10 millones de euros o el 2 % del volumen de negocios mundial anual** de la entidad infractora.

Asimismo, el Anteproyecto determina que los Directivos puedan responder solidariamente de los incumplimientos de su entidad, pudiendo llegar a hacerlo con su patrimonio personal frente a multas de millones de euros. Además, el Anteproyecto refuerza la estructura institucional mediante la creación de un **Centro Nacional de Ciberseguridad**, encargado de coordinar la respuesta ante incidentes y de servir como punto de contacto único con la Unión Europea.

### 3. ¿A qué entidades aplica la normativa NIS 2?

En términos generales, la norma se aplica a todas las entidades públicas o privadas pertenecientes a los sectores críticos definidos en la propia Directiva —ya sean **sectores de alta criticidad u otros sectores críticos**, según se detalla más adelante—, siempre que dichas entidades alcancen al menos la dimensión de una empresa mediana conforme a la Recomendación 2003/361/CE, de 6 de mayo de 2003.

Esto implica que quedan comprendidas dentro del ámbito de aplicación aquellas organizaciones de los referidos sectores que cuenten con **50 o más personas trabajadoras, o bien cuyo volumen de negocios anual o balance general anual supere los 10 millones de euros**.

Asimismo, la Directiva NIS2 extiende su ámbito de aplicación más allá del criterio general de tamaño (medianas o grandes empresas) en determinados supuestos en los que la naturaleza del servicio o su impacto potencial justifican una protección reforzada. En consecuencia, también quedarán sujetas a las obligaciones de la norma, con independencia de su dimensión, las entidades pertenecientes a sectores de alta o de otra criticidad cuando concurra alguno de los siguientes casos:

- En primer lugar, se incluyen los proveedores de redes públicas de comunicaciones electrónicas o de servicios electrónicos disponibles al público, así como los prestadores de servicios de confianza, los registros de nombres de dominio de primer nivel (TLD) y los proveedores de servicios de sistema de nombres de dominio (DNS).
- Asimismo, se consideran dentro del ámbito aquellas entidades que constituyan el único proveedor en un Estado miembro de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas, así como aquellas cuya interrupción del servicio pueda generar repercusiones significativas sobre la seguridad pública, el orden público o la salud pública.
- También se incluyen las entidades cuya perturbación pudiera inducir riesgos sistémicos relevantes, especialmente cuando tales efectos puedan tener repercusiones transfronterizas, y las que resulten críticas por su importancia específica a nivel nacional o regional, ya sea para su propio sector o para otros sectores interdependientes.
- De igual modo, NIS2 se aplica a las entidades de la Administración pública de ámbito central o regional que, de conformidad con el Derecho nacional, presten servicios cuya interrupción pudiera tener un impacto significativo en actividades sociales o económicas esenciales.
- La Directiva otorga además a los Estados miembros un margen de apreciación para incorporar al ámbito de aplicación a centros de enseñanza —en particular aquellos que desarrollen actividades críticas de investigación— y a la Administración pública local, cuando así lo determinen las autoridades competentes.

# Nota informativa

---

Por último, quedan igualmente comprendidas las entidades identificadas como críticas conforme a lo previsto en el artículo 2.1 de la Directiva (UE) 2022/2557 del Parlamento Europeo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas (CER), asegurando la coherencia entre ambos marcos normativos europeos.

## 3.1. Sectores de alta criticidad

- Agua potable
- Aguas residuales
- Banca
- Energía
- Espacio
- Gestión de servicios TIC (B2B)
- Infraestructura digital
- Infraestructuras de los mercados financieros
- Sector salud (tanto el sanitario como el farmacéutico)
- Transporte

## 3.2. Otros sectores críticos

- Fabricación, producción y distribución de sustancias y mezclas químicas
- Fabricación de determinados productos (sanitarios, informáticos y electrónicos, material eléctrico, maquinaria, vehículos a motor y material de transporte)
- Gestión de residuos
- Investigación
- Producción, transformación y distribución de alimentos
- Proveedores de servicios digitales (motores de búsqueda y redes sociales)
- Servicios postales y de mensajería

## 4. Deberes de gestión y supervisión: implicación directa de los órganos de dirección

Una de las principales innovaciones de NIS2 radica en la **responsabilidad directa del órgano de dirección** en la aprobación, supervisión y revisión de las medidas de ciberseguridad. Los administradores y consejeros deberán garantizar que las políticas de gestión de riesgos son adecuadas y que los equipos responsables disponen de los recursos y formación necesarios. La Directiva exige asimismo que los miembros del órgano de dirección reciban **formación específica en materia de ciberseguridad**, con el fin de asegurar una comprensión real de las amenazas y de las decisiones adoptadas en este ámbito. También les exige asegurarse de que el resto del personal de la entidad reciba formación en ciberseguridad.

## 5. Medidas de seguridad informáticas y notificación de incidentes y supervisión

La Directiva obliga a implementar un conjunto mínimo de medidas de seguridad de la información, tanto legales como informáticas y organizativas. Sin embargo, entre estas medidas se incluye un análisis de riesgos informáticos y la adopción de las correspondientes medidas de mitigación de impacto y probabilidad del riesgo por lo que, en sentido estricto, no todas las entidades tienen que adoptar exactamente las mismas medidas.

La Directiva impone también un **régimen de notificación escalonado** para los incidentes significativos de seguridad. Las entidades deberán comunicar una alerta temprana en el plazo de 24 horas, un informe intermedio en 72 horas y un informe final en el plazo máximo de un mes desde la detección del incidente.

# Nota informativa

## 6. Integración con el *compliance* penal y la jurisprudencia reciente

La NIS2 impone obligaciones de supervisión y medidas de ciberseguridad a los órganos de dirección, y es clave recordar que **el incumplimiento de estas obligaciones** puede conllevar sanciones administrativas, económicas e incluso **responsabilidad civil subsidiaria derivada del delito** (STS 699/2025, de 19 de febrero).

En este sentido, la jurisprudencia reciente del Tribunal Supremo ha reforzado esta idea al reconocer la **responsabilidad civil subsidiaria derivada del delito de las empresas por delitos virtuales vinculados a su sistema informático, cuando una deficiencia en sus medidas de seguridad facilita fraudes o daños a terceros**. En este contexto, la correcta implementación de las exigencias de NIS2 no solo contribuye al cumplimiento normativo, sino que también puede actuar como un elemento eximente en materia de responsabilidad civil derivada del delito.

De este modo, el cumplimiento de la normativa NIS2 no es solo una obligación legal y un elemento dirigido a la prevención de determinados delitos informáticos (como daños o protección de datos personales), sino que se convierte en un elemento clave dentro de un marco de estrategia global de defensa corporativa: **el sistema de *Corporate Compliance***.

## 7. Próximos pasos

A medida que avance la tramitación parlamentaria del Anteproyecto, las organizaciones deberán anticiparse, **evaluando su condición de entidad esencial o importante**, designando un responsable de seguridad y **adaptando sus políticas internas de gestión de riesgos y respuesta a incidentes**. La alineación entre los equipos técnicos, jurídicos y de cumplimiento será determinante para garantizar una implementación eficaz y evitar responsabilidades futuras. No es aconsejable que un único departamento gestione el cumplimiento de esta normativa, debiendo colaborar y coordinarse, como mínimo, los departamentos de legal, seguridad informática y cumplimiento normativo.

### ¿Tiene alguna consulta?

Desde las áreas de *Compliance* y de Derecho Digital y Protección de Datos trabajamos para poder dar respuesta a las dudas que la actual situación pueda plantear. Si tiene alguna consulta, no dude en ponerse en contacto con nosotros.

#### Contacto:

##### Íñigo de Ros Raventós

Socio del Área de Derecho  
Penal-Económico y Compliance  
[ideros@rcd.legal](mailto:ideros@rcd.legal)

##### David Molina

Director en el Área de Derecho  
Digital y Protección de Datos  
[dmolina@rcd.legal](mailto:dmolina@rcd.legal)

[www.rcd.legal](http://www.rcd.legal)