



Intech
Sistemas

GUÍA GRATUITA

NIS2 para pymes: qué es, a quién afecta y por dónde empezar

La directiva europea de ciberseguridad explicada sin tecnicismos, con la situación en España y ocho pasos prácticos para prepararte.

En resumen

- **La NIS2 es la directiva europea de ciberseguridad** que obliga a miles de empresas de sectores clave a gestionar sus riesgos y notificar sus incidentes.
- **En España todavía no hay ley que la aplique.** El proyecto de ley no llegó a tramitarse en las Cortes antes de su disolución en octubre de 2026, y el próximo Gobierno tendrá que retomarlo.
- **Afecta directamente a empresas medianas y grandes** de 18 sectores, y a algunas entidades sin importar su tamaño.
- **También llega a las pymes que son proveedoras** de esas empresas: la directiva les exige controlar la seguridad de su cadena de suministro.
- **Prepararse ahora es más barato que hacerlo con prisa:** las medidas que pide son, en gran parte, buenas prácticas que protegen a cualquier empresa.

Qué es la NIS2

La NIS2 es la [Directiva \(UE\) 2022/2555](#), aprobada en diciembre de 2022 para conseguir un nivel común y elevado de ciberseguridad en toda la Unión Europea. Sustituye a la primera directiva NIS, de 2016, y amplía mucho el número de empresas obligadas.

Su idea central es sencilla: las organizaciones que prestan servicios importantes para la sociedad deben **gestionar sus riesgos de ciberseguridad de forma organizada, avisar a las autoridades cuando sufren un incidente grave y implicar a su dirección**, que pasa a responder del cumplimiento.

Una directiva no obliga directamente a las empresas: cada país debe incorporarla a su legislación mediante una ley nacional. El plazo para hacerlo terminó el 17 de octubre de 2024.

Situación en España (octubre de 2026)

España aún no ha aprobado la ley que incorpora la NIS2, y la convocatoria de elecciones retrasa de nuevo su aprobación.

Fecha	Hito
29 nov. 2026	Elecciones generales. El nuevo Gobierno deberá volver a aprobar el anteproyecto en el Consejo de Ministros
6 oct. 2026	El Real Decreto 806/2026 disuelve las Cortes. El anteproyecto no se encontraba en tramitación parlamentaria
8 jul. 2026	La Comisión Europea lleva a España ante el Tribunal de Justicia de la UE por no haber incorporado la directiva
14 ene. 2025	El Consejo de Ministros aprueba el anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad
17 oct. 2024	Vence el plazo europeo para incorporar la NIS2 a la legislación nacional

Qué significa para tu empresa:

- Mientras no se publique la ley en el BOE, las obligaciones concretas de la NIS2 no son exigibles a la mayoría de empresas privadas.
- Sigue en vigor el Real Decreto-ley 12/2018, que incorporó la primera directiva NIS y ya obliga a los operadores de servicios esenciales.
- El anteproyecto prevé crear un Centro Nacional de Ciberseguridad como autoridad única. Su contenido final puede cambiar con el nuevo Gobierno.
- La presión europea para aprobarla es alta: conviene prepararse sin esperar a la publicación de la ley.

¿Afecta a mi empresa?

La NIS2 se aplica según dos criterios: el **sector** en el que trabaja la empresa y su **tamaño**.

Responde a estas preguntas en orden:

1. ¿Tu actividad está en uno de los 18 sectores de la directiva?

- *Sectores de alta criticidad (anexo I):* energía, transporte, banca, infraestructuras de los mercados financieros, sanidad, agua potable, aguas residuales, infraestructura digital, gestión de servicios TIC entre empresas, administración pública y espacio.
- *Otros sectores críticos (anexo II):* servicios postales y de mensajería, gestión de residuos, sustancias químicas, alimentación, fabricación (productos sanitarios, electrónica, equipos eléctricos, maquinaria y vehículos), proveedores de servicios digitales e investigación.

2. ¿Es una empresa mediana o grande? La directiva se aplica, con carácter general, a partir de empresa mediana según la definición europea: 50 trabajadores o más, o más de 10 millones de

euros de volumen de negocio anual y de balance.

3. **¿Está en la lista de excepciones?** Algunas entidades quedan incluidas sin importar su tamaño: proveedores de comunicaciones electrónicas, prestadores de servicios de confianza, registros de dominios y servicios DNS, y entidades que el Estado considere críticas por ser el único proveedor de un servicio esencial o por su impacto en la seguridad o la salud públicas.

Si se cumplen los criterios, la empresa será **esencial** o **importante**. Son esenciales, sobre todo, las grandes empresas de los sectores del anexo I; las demás incluidas serán importantes. Las dos categorías tienen las mismas obligaciones, pero las esenciales tienen una supervisión más estricta y sanciones más altas.

Si tu empresa es pequeña o no está en estos sectores, puede afectarte igualmente como proveedora. La directiva obliga a las entidades incluidas a vigilar la seguridad de su cadena de suministro y a valorar las prácticas de ciberseguridad de sus proveedores directos. En la práctica, pueden pedirte medidas, compromisos o evidencias por contrato.

La clasificación definitiva dependerá de la ley española, cuando se apruebe. Ante la duda, consulta tu caso concreto.

Qué exige

La directiva pide tres cosas: aplicar diez medidas de gestión de riesgos, implicar a la dirección y notificar los incidentes graves.

Las diez medidas mínimas (artículo 21)

Deben ser adecuadas y proporcionadas al tamaño de la empresa, a su exposición al riesgo y al coste de aplicarlas.

Medida	Qué significa en la práctica
Análisis de riesgos y políticas de seguridad	Saber qué sistemas y datos son críticos y qué podría fallar, y documentar cómo se protegen
Gestión de incidentes	Un procedimiento para detectar, contener y resolver incidentes
Continuidad de negocio	Copias de seguridad, recuperación ante desastres y gestión de crisis
Seguridad de la cadena de suministro	Valorar y exigir medidas de seguridad a proveedores directos
Seguridad en compras, desarrollo y mantenimiento	Mantener los sistemas actualizados y gestionar las vulnerabilidades
Evaluación de la eficacia	Revisar periódicamente si las medidas funcionan
Higiene básica y formación	Actualizaciones, contraseñas, copias y formación del personal
Criptografía	Cifrar la información cuando sea apropiado
Personas, accesos y activos	Inventario de equipos, permisos mínimos y altas y bajas controladas
Autenticación y comunicaciones seguras	Doble factor (MFA) y canales seguros, también para emergencias

La dirección responde (artículo 20)

Los órganos de dirección deben aprobar las medidas, supervisar su aplicación y pueden ser considerados responsables de su incumplimiento. Sus miembros están obligados a formarse en ciberseguridad, y se recomienda formar también a la plantilla con regularidad.

Notificación de incidentes significativos (artículo 23)

Un incidente es significativo si causa o puede causar una interrupción grave del servicio o pérdidas económicas, o daños considerables a otras personas o empresas. Hay que notificarlo al equipo nacional de respuesta (CSIRT) o a la autoridad competente:

Plazo desde que se conoce	Qué se envía
24 horas	Alerta temprana: qué ha pasado y si puede ser malicioso o afectar a otros países
72 horas	Notificación del incidente, con una primera valoración de su gravedad e impacto
A petición	Informes intermedios sobre su evolución
1 mes	Informe final: descripción, causa probable, medidas aplicadas e impacto

Cuando proceda, también hay que informar sin demora a los clientes afectados.

Sanciones

La directiva fija los importes máximos mínimos que cada país debe prever por incumplir las medidas o las obligaciones de notificación. Cada ley nacional puede establecer importes superiores.

Tipo de entidad	Multa máxima de, al menos
Esencial	10 millones de euros o el 2 % de la facturación mundial anual, la cantidad mayor
Importante	7 millones de euros o el 1,4 % de la facturación mundial anual, la cantidad mayor

Además de las multas, las autoridades pueden ordenar auditorías, inspecciones y medidas correctoras. En España, el régimen sancionador concreto dependerá de la ley que finalmente se apruebe.

Por dónde empezar

Ocho pasos que sirven tanto si la NIS2 te afecta directamente como si eres proveedor de una empresa afectada:

1. **Comprueba si estás incluido.** Revisa tu sector y tu tamaño con las preguntas de esta guía, y pregunta a tus clientes principales si van a exigirte medidas.
2. **Haz inventario.** Equipos, servidores, aplicaciones, servicios en la nube, datos críticos y quién tiene acceso a qué.

3. **Analiza los riesgos.** Qué es lo que más daño haría si fallara y qué probabilidad tiene de ocurrir.
4. **Asegura las copias.** Copias automáticas, al menos una aislada de la red, y pruebas de recuperación periódicas.
5. **Protege los accesos.** Doble factor en correo y accesos remotos, permisos mínimos y bajas de personal el mismo día.
6. **Mantén los sistemas al día.** Actualizaciones centralizadas y sustitución de los sistemas que ya no reciben parches.
7. **Prepara la respuesta.** Un plan breve que diga quién decide, a quién avisar, qué desconectar y cómo cumplir los plazos de 24 y 72 horas.
8. **Implica a la dirección y forma al equipo.** Que la dirección apruebe el plan y que la plantilla sepa reconocer correos fraudulentos.

Si quieres saber cómo estás hoy, prueba el [autodiagnóstico de ciberseguridad](#) de nuestra web: diez preguntas y un resultado inmediato, sin registro.

Fuentes y aviso legal

Guía actualizada a 26 de octubre de 2026. La situación legislativa en España puede cambiar tras las elecciones del 29 de noviembre de 2026; revisaremos esta guía cuando haya novedades.

- [Directiva \(UE\) 2022/2555 \(NIS2\)](#), [texto oficial en EUR-Lex](#): artículos 2 y 3 (ámbito), 20 (gobernanza), 21 (medidas), 23 (notificación) y 34 (multas).
- [Ministerio del Interior: aprobación del anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad \(14 de enero de 2025\)](#)
- [Mobile World Live: efectos de la disolución de las Cortes sobre las leyes tecnológicas \(6 de octubre de 2026\)](#)
- [DSI: estado de la NIS2 en España \(octubre de 2026\)](#)

Aviso: esta guía ofrece información general y divulgativa. No constituye asesoramiento jurídico ni sustituye el análisis de cada caso concreto. © 2026 INNOVA TECH SERVICIOS BARCELONA, S.L. (InTech Sistemas).

Cómo puede ayudarte InTech

En InTech Sistemas acompañamos a las empresas desde el diagnóstico hasta la verificación de las medidas, y todo queda por escrito.

Compliance RGPD, NIS2 y ENS

Diagnóstico de obligaciones y riesgos, plan de adecuación con prioridades y responsables, implantación y verificación con evidencias.

Acronis Cyber Protect · Gold Partner

Copias de seguridad, recuperación ante desastres, EDR y XDR, protección de datos (DLP) y gestión de equipos.

Tecnología propia

SentinelBlockIP, para bloquear los intentos de acceso por fuerza bruta en Windows, y los reportes diarios de copias, para saber cada mañana qué se ha copiado y qué ha fallado.



La consulta inicial no tiene coste

Nos cuentas tu situación, te planteamos alternativas y te las enviamos por escrito.

+34 668 57 23 91 · +34 668 57 23 87 · info@intechsistemas.com · intechsistemas.com