

# Directiva NIS2: requisitos más estrictos para la ciberseguridad

La directiva NIS2 es una normativa de ámbito comunitario cuyo objetivo es incrementar el nivel de ciberseguridad en la Unión Europea. Esto lo consigue, entre otras cosas, abordando una gama más amplia de industrias, exigiendo medidas de ciberseguridad más estrictas (incl. los riesgos de ciberseguridad en las cadenas de suministro) y creando requisitos más estrictos para los informes de incidentes.

Los estados miembros de la UE tienen hasta septiembre de 2024 para convertir la Directiva NIS2 en actos ejecutivos nacionales. Estos serán vinculantes por ley, lo cual significa que tu organización (si entra en el ámbito de aplicación) deberá cumplir con los requisitos.


















## Organizaciones incluidas en el ámbito de aplicación

La directiva NIS2 está destinada a organizaciones medianas o grandes, y ahora ofrece una lista ampliada de sectores sujetos a la normativa.

Las organizaciones se clasifican (en base a su tamaño y sector) como “entidades esenciales” o “entidades importantes”. Esta clasificación influye en las responsabilidades que tendrán las organizaciones cuando entre en vigor la NIS2.

*Nota: la directiva NIS2 enumera las excepciones a la regla del tamaño máximo y la clasificación por sectores.*

Véase [Capítulo 1 - Artículos 2 y 3](#)

Settore	Subsector	Gran tamaño Más de 250 empleados o Más de 50 millones de ingresos	Tamaño medio 50-250 empleados o 10-50 millones de ingresos
 Energía	electricidad, gas, petróleo, calefacción/refrigeración, hidrógeno y operadores de puntos de recarga de EV	Essenziale	Importante*
 Transportes	transportes por aire, ferrocarril, carretera y agua (incl. empresas navieras e instalaciones portuarias)	Esencial	Importante*
 Banca y finanzas	entidades de crédito, infraestructuras de los mercados financieros, centros de negociación y contrapartes centrales (atención: DORA)	Esencial	Importante*
 Salud	proveedores sanitarios, laboratorios de investigación, productos farmacéuticos y fabricantes de dispositivos médicos	Esencial	Importante*
 Agua	proveedores de agua potable y operadores de aguas residuales (sólo si forma parte esencial de su actividad general)	Esencial	Importante*
 Infraestructura digital y servicios informáticos	servicios de confianza, DNS, registros de nombres TLD y redes públicas de comunicaciones electrónicas	Esencial	Esencial
	intercambio de internet, centros de datos, computación en la nube y servicios gestionados (de seguridad)	Esencial	Importante*
 Administración pública	administración central (excl. poder judicial, parlamento, banco nacional, defensa, seguridad nacional / pública)	Esencial	Esencial
	gobierno regional: basado en el riesgo, gobierno local: opcional	Importante*	Importante*
 Espacio	operadores de infraestructuras terrestres	Esencial	Importante*
 Servicios postales y de mensajería		Importante*	Importante*
 Gestión de residuos	(sólo si es su actividad económica principal)	Importante*	Importante*
 Productos químicos	fabricación, producción y distribución	Importante*	Importante*
 Alimentación	producción, transformación y distribución	Importante*	Importante*
 Fabricantes	dispositivos médicos; ordenadores, electrónica, óptica, maquinaria, vehículos motorizados, remolques y otros equipos de transporte	Importante*	Importante*
 Proveedores digitales	tiendas virtuales, motores de búsqueda y plataformas sociales	Importante*	Importante*
 Organismos de investigación	(excluyendo instituciones educativas)	Importante*	Importante*

## Requisitos de gestión de riesgos de ciberseguridad

Cuando se implemente, NIS2 aumentará el esfuerzo (mínimo) que las organizaciones deberían dedicar a la ciberseguridad. En resumen, la directiva NIS2 establece requisitos para:

### Propiedad del riesgo

La administración tiene la responsabilidad directa de garantizar que los riesgos cibernéticos sean identificados, abordados y que se cumplan los requisitos. [Capítulo IV - Artículo 20](#)

### Control de riesgos

Tu organización debe implementar medidas de prevención y de mitigación, que reduzcan los riesgos y sus impactos. Por ejemplo, medidas adecuadas en torno a la gestión de incidentes, ciberseguridad en las cadenas de suministro, seguridad de las redes, control de acceso y encriptación.

### Continuidad de negocio

Tu organización debe considerar cómo garantizar la continuidad de negocio si se ve afectada por un ciberataque grave. Por ejemplo, la recuperación de sistemas, procedimientos de emergencia y creación de una organización de crisis.

### Notificación de incidentes

Las organizaciones deben asegurar que las autoridades sean informadas de manera adecuada. Entre otras cosas, hay un requisito estricto de que los incidentes graves se notifiquen dentro de 24 horas y se realice una evaluación inicial dentro de 72 horas. [Capítulo IV - Artículo 23](#)

Más concretamente, el Artículo 21 de la Directiva NIS2 enumera explícitamente las siguientes medidas técnicas, operativas y organizativas para gestionar los riesgos que se plantean para la seguridad de las redes y los sistemas informáticos, así como para prevenir o minimizar el impacto de los incidentes: [Capítulo IV - Artículo 21](#)

- a. políticas sobre análisis de riesgos y seguridad de los sistemas informáticos.
- b. gestión de incidentes.
- c. continuidad de negocio, como gestión de copias de seguridad, recuperación de desastres y gestión de crisis.
- d. seguridad de la cadena de suministro, incluidos los aspectos relacionados con la seguridad en las relaciones entre cada entidad y sus proveedores directos o proveedores de servicios.
- e. seguridad en la adquisición, desarrollo y mantenimiento de redes y sistemas informáticos, incluyendo la gestión y divulgación de vulnerabilidades.
- f. políticas y procedimientos para evaluar la eficacia de las medidas de gestión de los riesgos de ciberseguridad.
- g. prácticas básicas de ciberhigiene y formación en ciberseguridad.
- h. políticas y procedimientos sobre el uso de la criptografía y, cuando sea apropiado, del cifrado.
- i. seguridad de los recursos humanos, políticas de control de acceso y gestión de activos.
- j. el uso de autenticación multifactor o soluciones de autenticación continua, comunicaciones seguras de voz, vídeo y texto y sistemas seguros de comunicación de emergencia dentro de la entidad, cuando sea apropiado.

## Supervisión y aplicación

Las organizaciones clasificadas como Entidades Esenciales pueden estar sujetas a supervisión in situ y ex situ, incluyendo controles aleatorios y auditorías anuales y específicas, basadas en los resultados de la evaluación de riesgos o en la información disponible relacionada con los mismos.

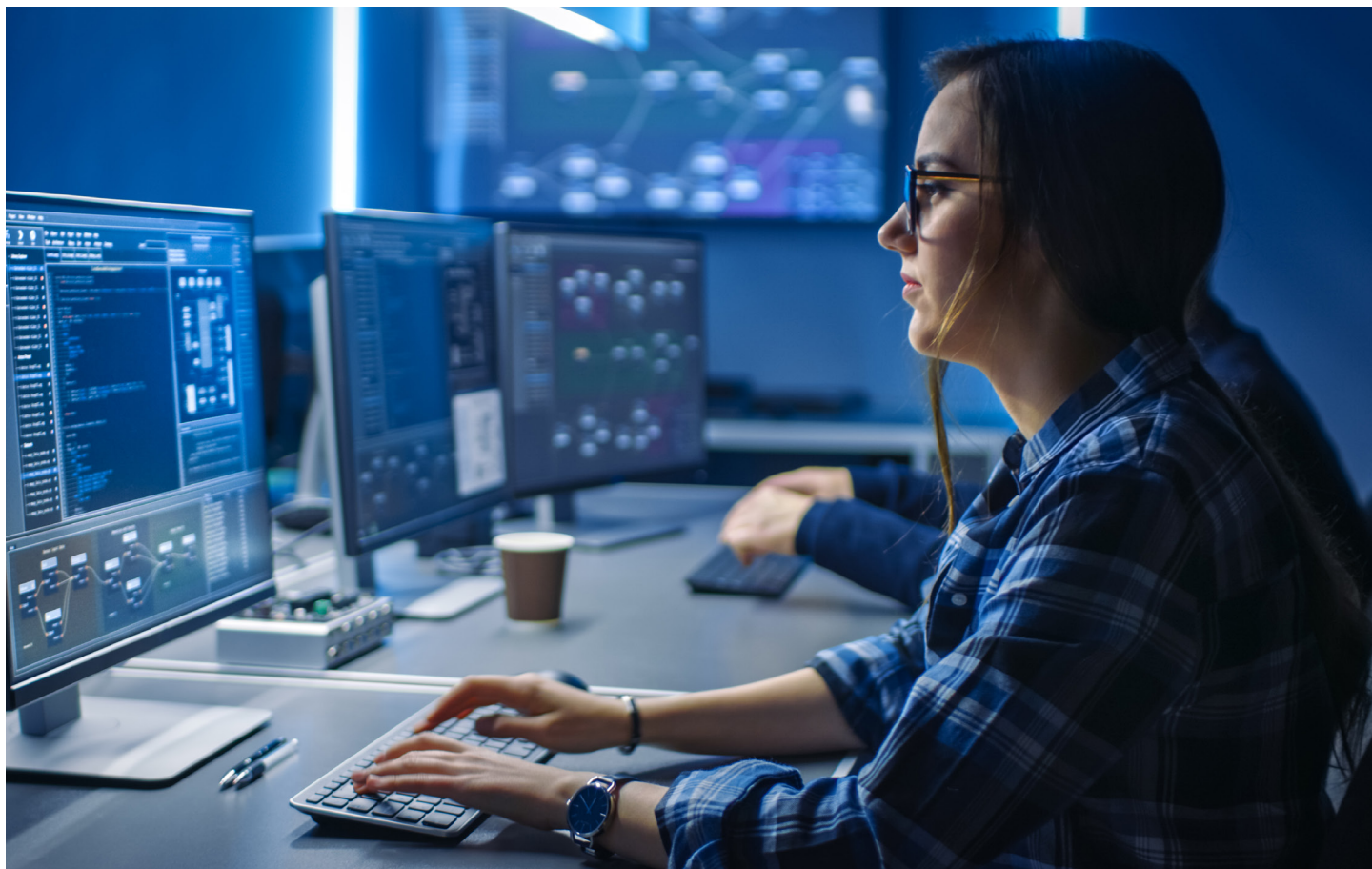
En virtud de la NIS2, las autoridades tienen el poder de responsabilizar personalmente a los directivos si se demuestra negligencia grave tras un ciberincidente. Para las Entidades Esenciales, las autoridades están facultadas a impedir temporalmente que una persona ejerza puestos gerenciales en caso de negligencia reiterada. [Capítulo VII - Artículo 32](#)

Las organizaciones clasificadas como Entidades Importantes estarán sujetas a una supervisión reactiva por parte de las autoridades, a diferencia de la supervisión proactiva reservada a las Entidades Esenciales. Esto significa que, a menos que exista un motivo para ello, como un ciberincidente o informes de organizaciones externas como auditores u otras partes de la cadena de suministro, una Entidad Importante no se enfrentará a la supervisión directa de reguladores y las autoridades.

[Capítulo VII - Artículo 33](#)


La directiva NIS2 amplía las sanciones, que ahora incluyen multas basadas en el volumen de negocios global. Estas sanciones se basan en si las organizaciones forman parte de una Entidad Esencial o Importante. Para las Entidades Esenciales, se basan en un mínimo de diez millones de euros, o el 2 % del volumen de negocios anual global, lo que resulte mayor.

Para las Entidades Importantes, las multas se basan en un mínimo de siete millones de euros o el 1,4 % del volumen de negocios. [Capítulo VII - Artículo 34](#)



## About Ivanti

Ivanti mejora y asegura el «Everywhere Work» para que las personas y las empresas puedan prosperar. Hacemos que la tecnología funcione para las personas, no al revés. Los empleados actuales utilizan una amplia gama de dispositivos corporativos y personales para acceder a aplicaciones y datos de TI a través de múltiples redes para mantenerse productivos dondequiera y comoquiera que trabajen. Ivanti es la única empresa tecnológica que encuentra, gestiona y protege cada activo de TI y punto final de una empresa. Más de 40 000 clientes, incluidos 88 de las compañías de Fortune 100, confían en Ivanti para poder ofrecer una excelente experiencia digital a sus empleados y mejorar la productividad y eficiencia de los equipos de TI y seguridad. En Ivanti, nos esforzamos por crear un entorno en el que se escuchen, respeten y valoren todas las perspectivas, y estamos comprometidos con un futuro más sostenible para nuestros clientes, socios, empleados y el planeta. Para obtener más información, visita [ivanti.com](https://www.ivanti.com)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

Para obtener más información,  
por favor visita [ivanti.com](https://www.ivanti.com)