¿Qué es la Directiva NIS2?

En la era digital actual, la ciberseguridad es una de las principales preocupaciones de particulares y organizaciones debido a la incidencia cada vez mayor de los ciberataques. Consciente de ello, la Comisión Europea introdujo la Directiva de Seguridad de las Redes y de la Información (NIS) de la UE en 2016 para mejorar la ciberseguridad en toda la Unión Europea. Sin embargo, la directiva carecía de responsabilidad, lo que llevó a la Comisión a planificar su sustitución por la directiva NIS2, más sólida.

La Directiva NIS2 obliga a las empresas a aplicar medidas clave de ciberseguridad, incluida la seguridad de la cadena de suministro, la criptografía y el cifrado (artículo 18). El artículo 89 hace hincapié en la adopción de prácticas básicas de ciberhigiene, como los principios de confianza cero, las actualizaciones de software, la configuración de dispositivos, la segmentación de redes y la gestión de identidades y accesos para entidades esenciales e importantes.

NIS frente a NIS2: ¿qué ha cambiado?

Hay algunas diferencias importantes entre la anterior y la nueva Directiva:

- La nueva propuesta elimina la distinción entre Operadores de Servicios Esenciales (OES) y Proveedores de Servicios Digitales (DSP), clasificando en su lugar a las entidades como esenciales o importantes.
- Se amplía el ámbito de aplicación de la Directiva para abarcar nuevos sectores en función de su grado de criticidad para la economía y la sociedad, incluyendo a todas las empresas medianas y grandes de estos sectores. Los Estados miembros también pueden identificar entidades más pequeñas con un perfil de alto riesgo
- Se propone la creación de una Red Europea de Organizaciones de Enlace para Crisis Cibernéticas (EU-CyCLONe) para trabajar colectivamente en la preparación y aplicación de planes de respuesta rápida de emergencia, por ejemplo en caso de un incidente o crisis cibernética a gran escala
- Mayor coordinación en la divulgación de nuevas vulnerabilidades descubiertas en toda la Unión. Se establece una lista de sanciones administrativas (similares a las del GDPR), incluidas multas por infringir las obligaciones de información y gestión de riesgos de ciberseguridad
- La Directiva NIS2 impone obligaciones directas a los órganos de dirección para aplicar y supervisar el cumplimiento de la legislación por parte de su organización, lo que puede dar lugar a multas y a la prohibición temporal de ejercer funciones de dirección, incluso a nivel de alta dirección

Además, introduce disposiciones más precisas sobre el proceso de notificación de incidentes, el contenido de los informes y el plazo (dentro de las 24 horas posteriores a la detección del incidente). A escala europea, la propuesta refuerza la ciberseguridad de las principales tecnologías de la información y la comunicación. Los Estados miembros, en cooperación con la Comisión y la Agencia de Ciberseguridad de la Unión Europea (ENISA), tendrán que llevar a cabo evaluaciones de riesgo coordinadas de las cadenas de suministro críticas.

¿A quién se aplica?

Mientras que con la antigua Directiva NIS los Estados miembros eran responsables de determinar qué entidades cumplían con los criterios para ser calificados como operadores de servicios esenciales, la nueva Directiva NIS2 introduce una regla de tamaño límite. Esto significa que **todas las entidades medianas y grandes que operen en los sectores o presten servicios cubiertos por la directiva entrarán en su ámbito de aplicación**.

A continuación, encontrará una clasificación según la regla de tamaño límite:

Entidades Esenciales (EE) Umbral de tamaño: varía según el sector, en general son 250 empleados, un volumen de negocios anual de 50 millones de euros o un balance de 43 millones de euros	**Entidades importantes (EI)** Umbral de tamaño: varía según el sector, pero generalmente son 50 empleados, un volumen de negocios anual de 10 millones de euros o un balance de 10 millones de euros
Energía	Servicios de correos
Transporte	Gestión de residuos
Finanzas	Productos químicos
Administración Pública	Investigación
Sanidad	Alimentación
Aerospacial	Producción
Suministro de agua (agua potable & aguas residuales)	Servicios digitales (redes sociales, motores de búsqueda, marketplaces etc.)
Infraestructura digital (por ejemplo, proveedores de servicios de computación en la nube y gestión de las TIC)	

La Directiva NIS2 también cubre los organismos de la administración pública a nivel central y regional, pero excluye a los parlamentos y los bancos centrales.

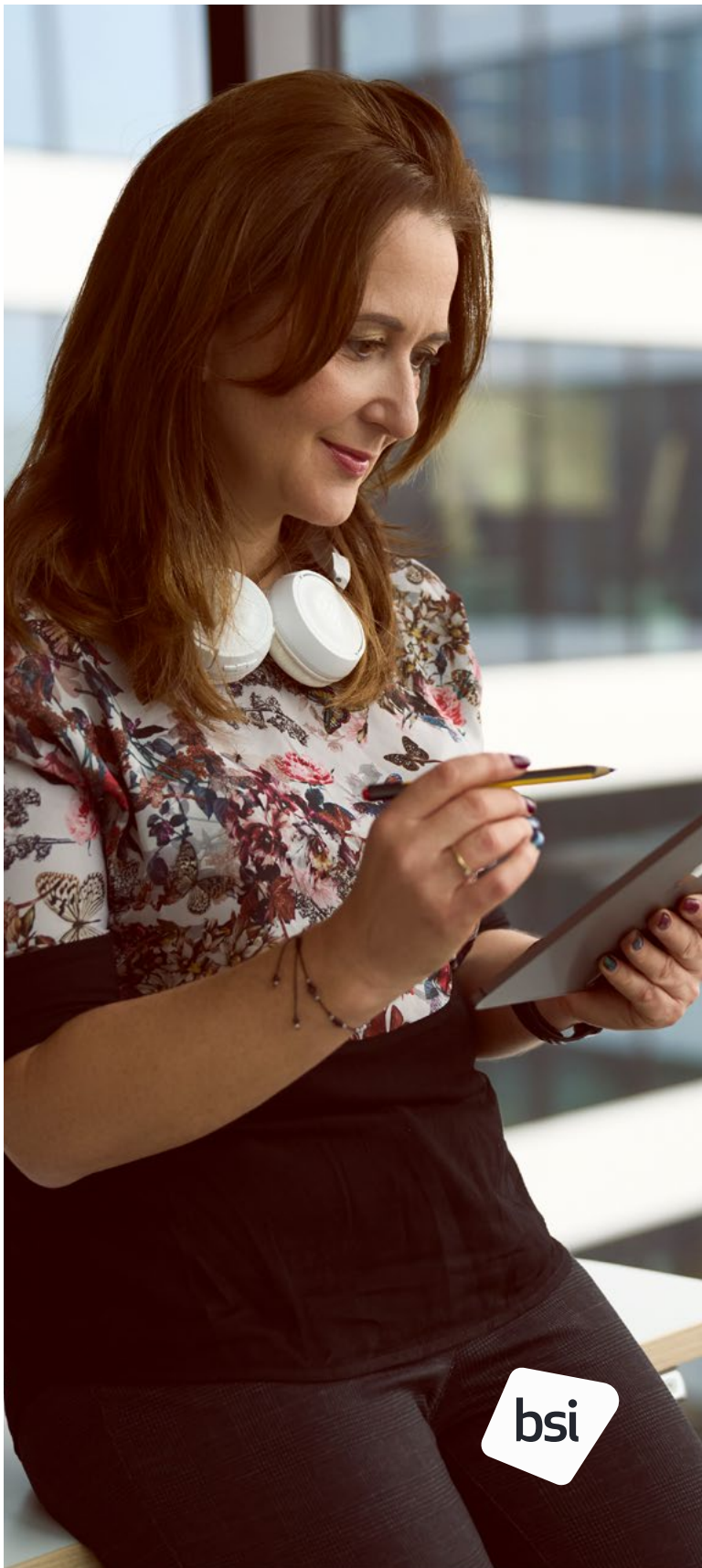
¿Cuándo entrará en vigor?

Todos los Estados miembros de la UE deben incorporar las nuevas obligaciones a sus legislaciones nacionales antes del 17 de octubre de 2024. Tras la aprobación definitiva el 16 de enero de 2023, se ha concedido a las entidades cubiertas un plazo de cumplimiento de 21 meses una vez que la directiva entre en vigor. La siguiente lista muestra el calendario de desarrollo de la Directiva NIS:

- **6 de julio de 2016:** Adopción de la Directiva
- **9 de mayo de 2018:** Fecha límite para que los Estados miembros transpongan la Directiva NIS a la legislación nacional
- **7 de julio de 2020:** La Comisión Europea inicia una consulta sobre la reforma de la Directiva NIS
- **16 de diciembre de 20201:** La Comisión Europea publica la propuesta de la Directiva NIS2
- **22 de noviembre de 2021:** El Parlamento Europeo adopta su postura negociadora
- **3 de diciembre de 2021:** El Consejo Europeo adopta su postura negociadora
- **13 de enero de 2022:** Primera ronda de negociaciones a tres bandas
- **16 de febrero de 2022:** Segunda ronda de negociaciones a tres bandas
- **13 de mayo de 2022:** Se alcanza un acuerdo político
- **10 de noviembre de 2022:** El Parlamento Europeo vota la adopción de la Directiva NIS2
- **28 de noviembre de 2022:** La Directiva NIS2 aprobada por el Consejo de la UE
- **27 de diciembre de 2022:** La Directiva NIS2 es publicada en el Diario Oficial y entra en vigor 20 días después, el 16 de enero de 2023
- **17 de octubre de 2024:** Fecha límite para que los Estados miembros incorporen la Directiva NIS2 a su legislación nacional

¿Cómo podemos ayudar a su empresa a cumplir con la normativa NIS2?

En BSI, contamos con un amplio equipo de expertos con gran experiencia y líderes en el sector que le ayudarán a garantizar que usted y su empresa cumplan con todos los requisitos de seguridad necesarios para poder anticiparse a la Directiva NIS2. Con nuestra ayuda, las organizaciones pueden evitar posibles sanciones económicas e inspirar aún más confianza entre sus clientes. Desde la identificación inicial de OES hasta la autoevaluación, la evaluación de riesgos y el tratamiento de riesgos, nuestra experiencia de trabajo con organizaciones de todos los sectores puede ayudarle en su proceso hacia el cumplimiento de la Directiva NIS2.



BSI ofrece actualmente los siguientes servicios en relación con los requisitos de la Directiva NIS2:

- Estrategia y gobernanza cibernética
- Evaluaciones de la situación e integridad de la ciberseguridad con respecto a los marcos estándar del sector
- Seguridad de la información/desarrollo de la estrategia cibernética/presentaciones a la junta directiva
- Gap analysis y apoyo a la implantación (ISO 27001, SOC 2, NIST CSF/800-53)
- Concienciación y formación en seguridad de la información Continuidad empresarial (ISO 22301)

Gestión de crisis y respuesta a incidentes

- Continuidad del Negocio (ISO 22301)
  - Análisis de Impacto en el Negocio (BIA), Desarrollo de Políticas, Planificación de la Continuidad del Negocio
- Soporte para Recuperación ante Desastres, Implantación y Pruebas Periódicas
- Pruebas de Penetración Basadas en Amenazas (pruebas pen)
- Inteligencia de Fuente Abierta (OSINT)
- Evaluaciones de Seguridad Física y Servicios de Simulación de Ataques (Red Teaming/ Blue Teaming y Purple Teaming)
- Planificación e Implantación de Respuesta a Incidentes (ISO27035)
  - Modelado de Amenazas/Evaluaciones de Amenazas
  - Evaluación de la capacidad actual de planificación y reporte de respuesta a incidentes
  - Pruebas de respuesta a incidentes/formación de personal

Gestión y Reporte de Riesgos

- Desarrollo e Implantación del Marco de Gestión de Riesgos de TI (ISO 27005)
- Gestión de Riesgos de Terceros (ISO 27036-2)
  - Evaluación del estado actual de la gestión del ciclo de vida de terceros
  - Desarrollar un marco de gestión integral de proveedores
  - Implantación del marco de gestión de riesgos de terceros junto con el soporte continuo de gestión de riesgos
- BSI trabaja con socios tecnológicos que ofrecen herramientas para facilitar la gestión completa del ciclo de vida de proveedores
  - Inteligencia de Amenazas/Equipo de Respuesta a Emergencias Informáticas (CERT) Certificación
  - Evaluar la posición actual y determinar el estado futuro
  - Crear un marco de reporte

¿Por qué las normas ISO 27001 e ISO 22301 son claves para el cumplimiento de la Directiva NIS2?

Las regulaciones NIS recomiendan que las empresas, en sus esfuerzos de cumplimiento, prioricen "el cumplimiento con estándares internacionales". Además, las directrices técnicas de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) alinean cada objetivo de seguridad con estándares de mejores prácticas, como la norma ISO 27001.

De todos los servicios que BSI puede ofrecer a su empresa en relación con la Directiva NIS2, dos normas parecen ser clave: la norma ISO 27001 y la norma ISO 22301.

- La implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001 capacita a las organizaciones para minimizar riesgos y exposición a amenazas de seguridad. Implica identificar políticas necesarias, emplear tecnologías adecuadas y proporcionar formación al personal para prevenir errores. Al exigir evaluaciones de riesgos anuales, la norma ISO 27001 permite a las organizaciones abordar proactivamente el panorama de riesgos en constante evolución.
- La norma ISO 27001 no solo facilita el cumplimiento de los requisitos de la Directiva NIS2, sino que también permite a las organizaciones obtener una certificación auditada de forma independiente. Esta certificación sirve como evidencia tangible para proveedores, partes interesadas y reguladores, demostrando la adopción de medidas técnicas y organizativas "apropiadas y proporcionadas" y estableciendo una ventaja competitiva en el mercado.
- Para las organizaciones que buscan un enfoque mejorado, se recomienda además la norma ISO 22301 para la gestión de la continuidad del negocio. La norma ISO 22301 ayuda en la implantación, mantenimiento y mejora continua de las prácticas de continuidad del negocio. Mientras que la norma ISO 27001 incorpora aspectos de la gestión de la continuidad del negocio (GCN), la norma ISO 22301 proporciona un proceso definido para la implantación de GCN. La certificación conforme a la norma ISO 22301 refuerza aún más el cumplimiento con la Directiva NIS2.

La sinergia entre la norma ISO 27001 y la norma ISO 22301 permite a las organizaciones desarrollar un sistema de gestión integrado que abarque tanto un SGSI como un SGCN. Este enfoque holístico no solo ayuda a cumplir las normas, sino que también fomenta el desarrollo de una sólida ciberresiliencia.

¿Por qué elegir BSI?

En BSI, nuestras competencias de primera clase transmiten confianza en los clientes en el ámbito de la ciberseguridad e higiene. Ofrecemos una sólida experiencia en ciberseguridad, gestión de riesgos y resiliencia de la información, con una perspectiva intersectorial global. Nuestros conocimientos abarcan cuestiones que afectan al sector público, las amenazas emergentes y la experiencia práctica del sector en la gestión del riesgo cibernético y la resiliencia.

¿Qué debe hacer a continuación?

- Verifique si su organización entra en el ámbito de aplicación
- Informe a su dirección o consejo de administración de la próxima entrada en vigor de la normativa
- Póngase en contacto con nosotros para que le ayudemos a cumplir con la normativa NIS2
  sales.es@bsigroup.com