NIS2:

¿PREPARADOS?

La guía completa para comprender los principios y obligaciones fundamentales de la nueva directiva europea sobre ciberseguridad, con consejos prácticos para crear un plan de acción eficaz y asegurarte de que lo tienes todo preparado.

Insight te ayuda
a empezar...

NIS2: un breve resumen

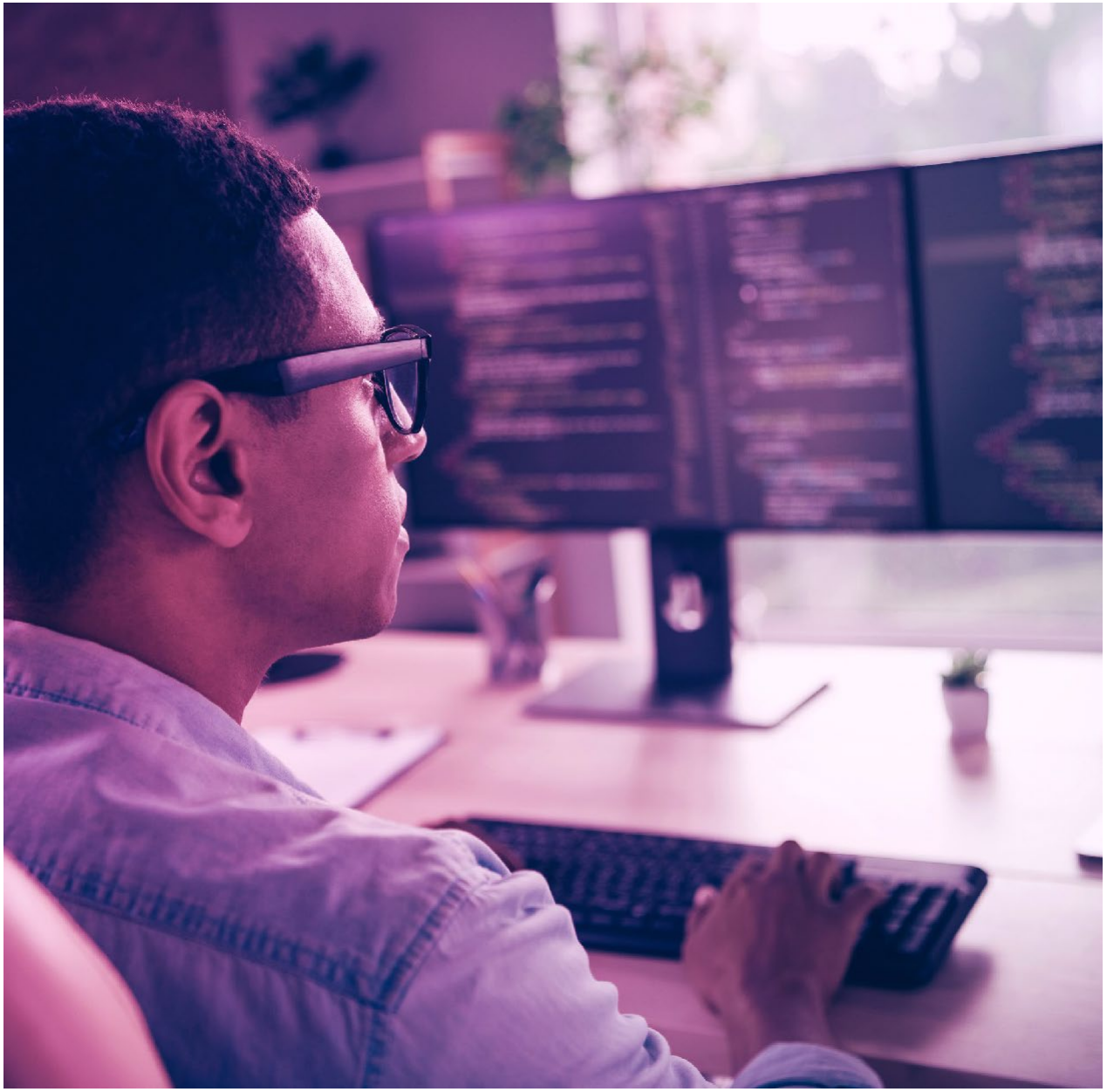
La Unión Europea (UE) ha elaborado la normativa NIS2 para mejorar la ciberseguridad y la ciberresiliencia. Los Estados miembros tienen hasta el 17 de octubre de 2024 para incorporar las medidas NIS2 a la legislación nacional, que las organizaciones deben cumplir.

NIS2 se aplica a las entidades «esenciales» e «importantes» en determinados sectores de cierto tamaño. Asimismo, también deberán cumplirla otros partners y organizaciones. La ley incluye responsabilidades como el deber de diligencia, la obligación de informar y la supervisión. El deber de diligencia exige que las organizaciones hagan sus propias evaluaciones de riesgos y tomen medidas para garantizar la seguridad y continuidad digitales. En virtud de la obligación de notificación, los incidentes deben notificarse en un plazo de 24 horas si se produce una interrupción del servicio. La supervisión incluye controles proactivos y reactivos para entidades clave. En caso de no hacerlo, se pueden imponer multas, siendo los directores responsables personales y solidarios de las infracciones.

Es crucial que todas las organizaciones, incluso las no afectadas directamente por NIS2, evalúen críticamente su resistencia frente a las amenazas. Todas las organizaciones se enfrentan a riesgos como el daño a la reputación, el robo de datos y las pérdidas financieras. La aplicación de las directrices de NIS2 constituye un excelente punto de partida para reforzar y mejorar continuamente las medidas de ciberseguridad.

Entendiendo NIS2

NIS2 es la nueva directiva europea sobre seguridad de las redes y de la información, que sustituye a la directiva NIS de 2018. Entrará en vigor en octubre de 2024. El objetivo de NIS2 es doble: armonizar las prácticas de ciberresiliencia en toda Europa y mejorar la ciberseguridad de empresas y organizaciones. A diferencia de las primeras directrices sobre NIS, que sólo se centraban en los sectores esenciales como el agua, la energía y las telecomunicaciones, la NIS2 se aplicará a una gama más amplia de organizaciones.



"Para cumplir las directrices de NIS2, es preciso determinar qué sistemas y servicios de su organización se consideran infraestructuras críticas y evaluar los riesgos asociados. Una vez que cuente con esta información, podrá adoptar las medidas necesarias a aplicar y saber cómo integrarlas en su organización."

Dirk de Goede, especialista en seguridad de Insight

¿A quién se aplica la directiva NIS2?

La directiva NIS2 clasifica las organizaciones en función de su sector y de su importancia para la sociedad y la economía. Distingue así entre dos tipos de entidades: entidades «esenciales» e «importantes», con disposiciones adicionales para casos especiales, como los proveedores de la cadena de suministro.

Entidades esenciales:	Sectores importantes
Energía	Servicios postales de mensajería
Infraestructura para el mercado financiero	Industria alimenticia
Infraestructura digital	Gestión de residuos
Servicios públicos	Proveedores digitales
Salud	Industria
Bancos	Productos químicos
Logística	Investigación
Administradores de servicios TI	
Agua potable	
Viajes espaciales	
Aguas residuales	

Los siguientes criterios permiten determinar si NIS2 es aplicable a su organización:

Entidades esenciales:

Grandes organizaciones con más de 250 empleados, una facturación superior a 50 millones de euros y un balance total superior a 43 millones de euros. Son cruciales para la economía y la sociedad, y el gobierno las supervisa activamente.

Entidades importantes:

Organizaciones medianas del grupo de entidades esenciales y organizaciones medianas a grandes en otros sectores clave. Estas entidades tienen al menos 50 empleados o una facturación anual y un balance total superior a 10 millones de euros. Se enfrentan a una supervisión menos estricta, pero se auditarán si hay señales de incumplimiento o después de un incidente.

Además, NIS2 se aplicará a:

- **Algunas organizaciones pequeñas**
- **Proveedores de la cadena de suministro de entidades esenciales e importantes**
- **Otras excepciones**

¿Cuáles son las obligaciones recogidas en la directiva NIS2?

NIS2 incluye tres obligaciones principales:

Deber de diligencia

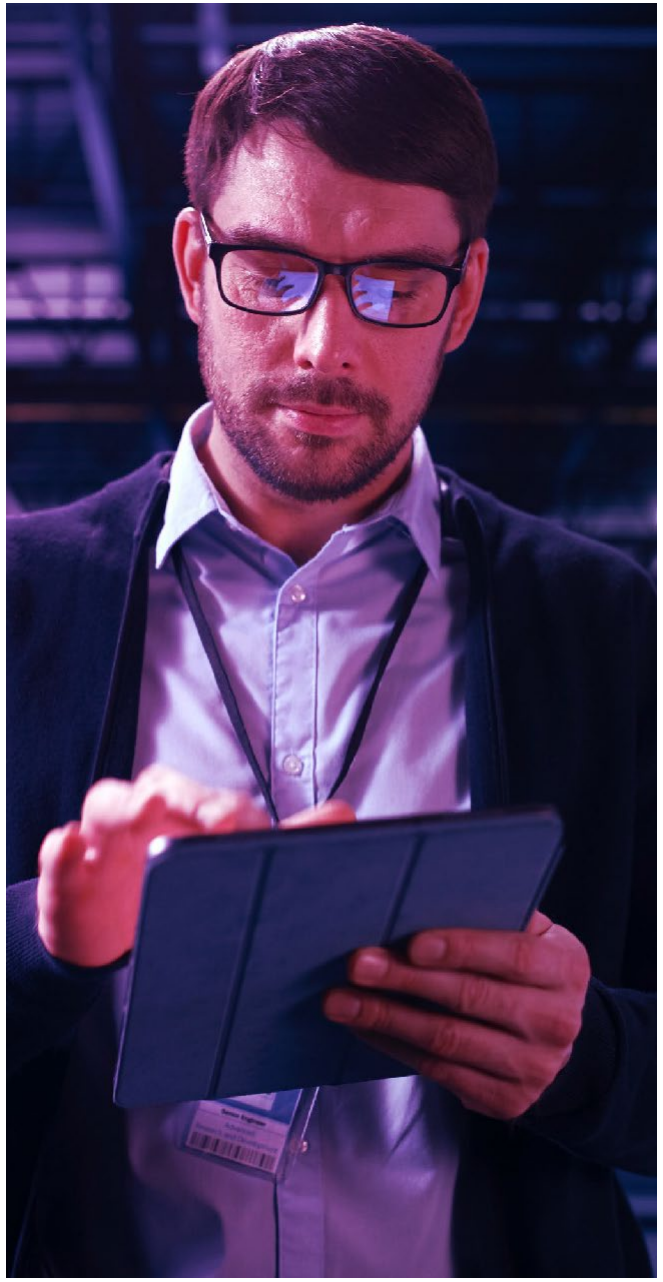
Las organizaciones deben realizar sus propias evaluaciones de riesgos y aplicar medidas para asegurar sus servicios y proteger la información.

Notificación de incidentes

Las organizaciones deben notificar a la autoridad supervisora los incidentes que puedan interrumpir significativamente los servicios esenciales en un plazo de 24 horas. Los incidentes cibernéticos también deben notificarse al Equipo de respuesta a incidentes de seguridad informática (CSIRT). Factores como la duración de la interrupción, el número de personas afectadas y las posibles pérdidas financieras determinan la necesidad de informar de un incidente.

Supervisión

Las organizaciones deben adherirse a estrictas obligaciones de supervisión, incluidas evaluaciones periódicas de sus medidas de ciberseguridad y prácticas de gestión de riesgos. También deben cooperar con las autoridades pertinentes y proporcionar actualizaciones oportunas sobre incidentes significativos o cambios que afecten a su seguridad.



¿Qué pasa si no se cumple?

Una vez que la Directiva NIS2 se haya transpuesto a la legislación de su país, todas las organizaciones incluidas en las categorías especificadas y casos especiales deberán cumplirla. En función de la clasificación de la organización, los controles de conformidad pueden realizarse de forma proactiva o reactiva.

Multas:

Si una organización incumple la norma NIS2, la autoridad supervisora puede imponer una multa tras una inspección. Cada Estado miembro establece sus propias multas, pero las máximas son:

- **Para organizaciones esenciales:** Hasta 10 millones de euros o el 2 % de la facturación anual global
- **Para organizaciones importantes:** Hasta 7 millones de euros o el 1,4% de la facturación anual global

Responsabilidad solidaria:

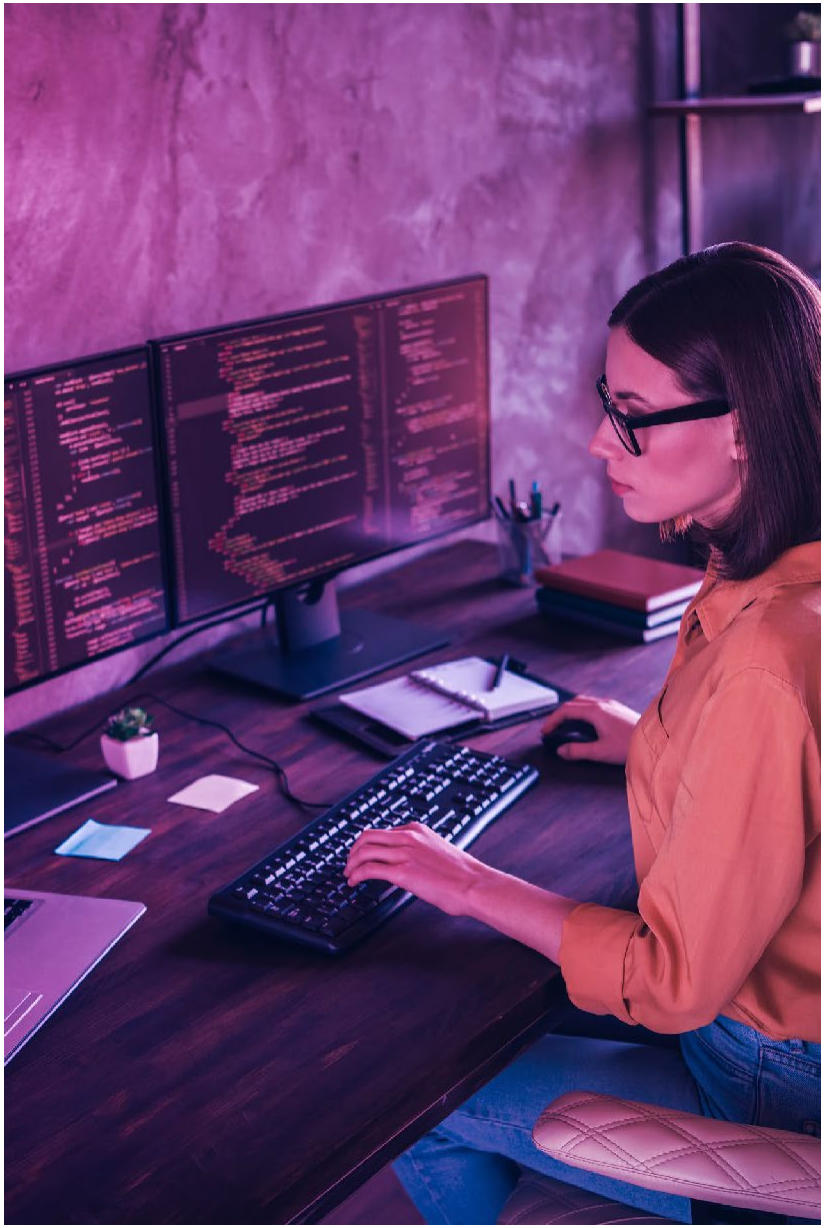
Cada director es personalmente responsable de garantizar que su organización cumple la norma NIS2. No pueden transferir esta responsabilidad ni culpar a otros de los posibles fallos.

Requisitos mínimos NIS2 para la gestión de riesgos de ciberseguridad

El artículo 21 de la Directiva NIS2 contiene una lista de medidas de gestión de riesgos de ciberseguridad que las entidades esenciales e importantes deben aplicar para proteger sus redes y sistemas de información.

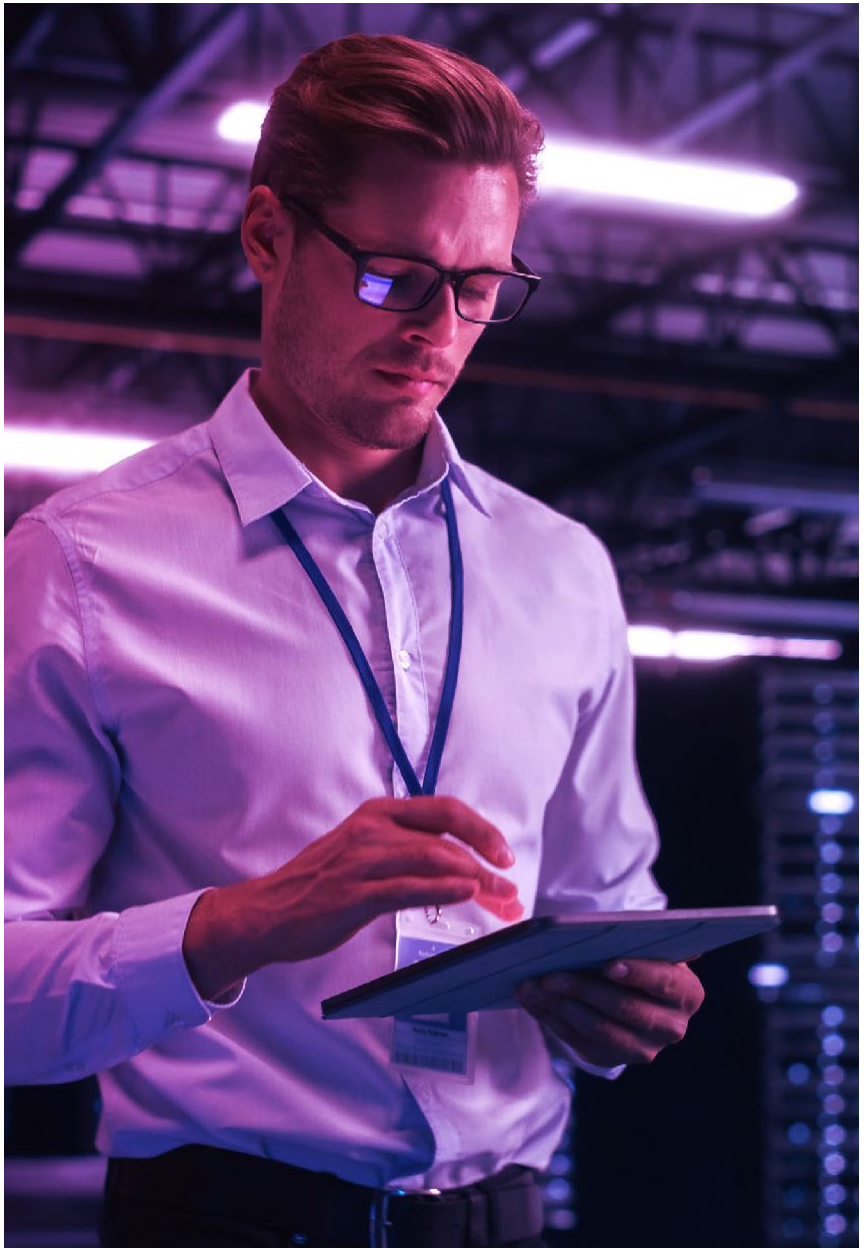
Requisitos mínimos de la norma NIS2:

1. **Análisis de riesgos:** ¿Qué sistemas y servicios son los más vitales para su organización y, por tanto, plantean el mayor riesgo? ¿Cómo se organiza la seguridad de su entorno?
2. **Continuidad del negocio** ¿Qué procedimientos existen para la gestión de incidentes, incluido un sólido sistema de copias de seguridad? ¿Qué medidas de gestión de crisis y recuperación se implementan?
3. **Seguridad de redes y sistemas de información:** ¿Cómo están configurados sus sistemas y cómo se abordan las vulnerabilidades?
4. **Eficacia:** ¿Cómo se comprueba la eficacia de sus medidas de seguridad? ¿Existen procedimientos establecidos para ello?
5. **Plan de respuesta a incidentes de seguridad:** ¿Cómo se gestionan y registran los incidentes?
6. **Seguridad de la cadena de suministro:** ¿A qué riesgos potenciales se enfrenta su organización con respecto a proveedores externos y proveedores de servicios?
7. **Concienciación sobre seguridad** ¿Cómo se gestiona la seguridad de su personal? ¿Todo el mundo conoce y cumple la política de seguridad? ¿Qué formación se ofrece al staff?
8. **Criptografía y cifrado** ¿Qué políticas y procedimientos existen en relación con el uso de criptografía y cifrado?
9. **Identidad y acceso:** ¿Cuáles son los aspectos de seguridad relacionados con el personal, las políticas de acceso y la gestión de activos?
10. **Autenticación multifactor** ¿Está implantada la autenticación multifactor para las cuentas accesibles desde Internet, las que tienen derechos administrativos y los sistemas esenciales?



Tu checklist para NIS2

Es importante no centrarse únicamente en los requisitos mínimos. En Insight sabemos que una evaluación NIS2 exhaustiva requiere información más detallada. Se recomienda la siguiente lista de comprobación de 25 elementos para garantizar el pleno cumplimiento y preparación de las medidas de la NIS2.



Cómo puede ayudar Insight

Entendemos que prepararse para la entrada en vigor de NIS2 es una operación importante para muchas organizaciones, y estamos aquí para ayudar. Si tienes alguna pregunta sobre NIS2 o necesitas más información sobre las medidas de nuestra checklist, no dudes en ponerte en contacto con nosotros.

Insight ofrece un enfoque integrado para lograr el cumplimiento normativo de la NIS2. Nos basamos en tus procesos actuales y garantizamos la armonización con otras directivas y reglamentos de la UE, para que la transición sea lo más fluida posible.

Mira el vídeo para descubrir cómo podemos ayudarte.

Acción inmediata

¿Busca asesoramiento inmediato para tu caso concreto? Insight ofrece diversos servicios, como el Workshop de concienciación sobre NIS2 o el Servicio de evaluación de NIS2, para proporcionarte una ventaja en el cumplimiento de los próximos requisitos de la normativa. Juntos, nos aseguraremos de que tu infraestructura de TI esté segura y de que tus datos empresariales estén protegidos.

Cada país tiene su propio Centro Nacional de Ciberseguridad para dar soporte y coordinar la implementación de la nueva directiva NIS2. Enlaces útiles a recursos locales del país para NIS2:

Austria

Punto de contacto NIS - Punto de contacto NISG

parlament.gv.at/asunto/XXVII/A/4129

Alemania

NIS2 en Alemania (NIS2UmsuCG) - OpenKRITIS

Directiva NIS 2, transposición en Alemania (NIS-2-directive.com)

Países Bajos

2,5 Mejorar la ciberseguridad - Gobierno digital (nldigitalgovernment.nl)

Bélgica

NIS2 | Centro de ciberseguridad de Bélgica

Italia

Autoridad y sanciones - ACN

España

Leyes clave de privacidad de datos y ciberseguridad | España | Manual global de privacidad de datos y ciberseguridad | Centro de recursos de Baker McKenzie

Adopción de la Directiva NIS2 | INCI-

Francia

https://cyber.gouv.fr/en

Irlanda

https://www.ncsc.gov.ie/

Reino Unido

(aunque no le afecta directamente, el Reino Unido tiene previsto evolucionar su actual normativa sobre NIS)

Respuesta del Gobierno a la convocatoria de propuestas para mejorar la ciberresiliencia del Reino Unido - GOV.UK (www.GOV.UK)

El marco de sistemas de red e información (NIS) tiene como objetivo mejorar la resiliencia a la ciberseguridad de

Da el siguiente paso

Confía en Insight para que te ayude a cumplir tus obligaciones NIS2. Te ofrecemos asesoramiento detallado y medidas prácticas que tu empresa puede necesitar para prepararse para la NIS2.

Visita es.insight.com y pónte en contacto con tu representante de cuenta para obtener recursos y asistencia adicionales.

MKT7148