NIS 2

Entendiendo NIS2: implicaciones y estrategias para la industria

5 DICIEMBRE 2025

EOHM Engineering Solutions

CONTENIDO

1 - ¿Qué es NIS2?

La Directiva NIS2 es el marco regulatorio europeo diseñado para aumentar de forma homogénea en todos los miembros de la unión la resiliencia cibernética de organizaciones críticas. Sustituye a la Directiva NIS1 y amplía tanto el alcance como los requisitos, reflejando la creciente exposición de los sistemas industriales a ciberataques.

"NIS2 no es solo una obligación legal: es un impulso estratégico hacia la resiliencia operativa."

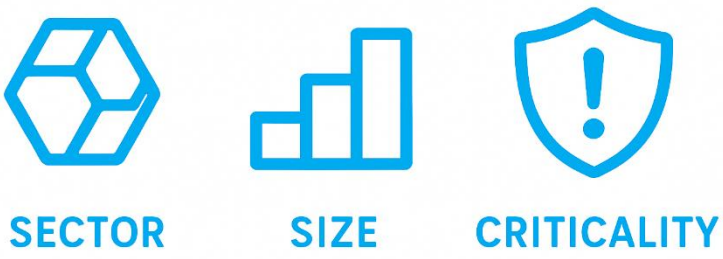
El objetivo de NIS2 es garantizar que los servicios vitales de cada organización se mantengan operativos frente a incidentes cibernéticos. En la industria, esto implica proteger no solo los sistemas de información tradicionales (IT), sino también los sistemas de control (OT), como PLCs, SCADA, sensores y redes de comunicación industriales, cuya interrupción puede afectar a la producción, la seguridad del personal, la calidad del producto e incluso el medio ambiente.

Los ciberataques ya no se restringen a IT, y la convergencia IT/OT junto con la digitalización de procesos han ampliado enormemente la superficie de ataque. Incluso el aislamiento tradicional de sistemas críticos mediante airgap ya no garantiza protección frente a amenazas modernas, como accesos remotos, dispositivos conectados o malware avanzado. Por ello, NIS2 establece la necesidad de demostrar de forma estructurada que se gestionan los riesgos y que la operación industrial es resiliente frente a incidentes.

En definitiva, NIS2 no se limita al cumplimiento legal y refuerza la idea de que la ciberseguridad industrial debe abordarse como un factor estratégico, protegiendo los sistemas críticos no solo para cumplir la normativa, sino para garantizar la continuidad, la seguridad y la reputación de las operaciones industriales.

2 - ¿Afecta a mi organización?

No todas las organizaciones están dentro del alcance de NIS2, pero la directiva amplía significativamente los sectores y organizaciones obligadas a cumplir. Para entornos industriales, los factores clave son: **sector, tamaño y criticidad de los sistemas.**



Autoevaluación

¿Has sido notificado como entidad esencial?

SI → Soy Entidad Esencial

NO → ¿La organización tiene más de 50 trabajadores?

SI → Soy Entidad Esencial

NO → ¿La organización factura más de 10M€?

SI → Soy Entidad Esencial

NO → ¿Realiza alguna actividad incluida en el Anexo I?

SI → Soy Entidad Esencial

NO → ¿Realiza alguna actividad incluida en el Anexo II?

SI → Soy Entidad Importante

NO → No me aplica

puedes formar parte de la cadena de suministro de organizaciones que sí están afectadas. En esos casos, los requisitos y expectativas de seguridad pueden trasladarse a tu operación de manera indirecta

Sector industrial Anexo I

- Energía
- Aguas Residuales
- Agua Potable
- Sanitario / Farma
- Transporte

Sector industrial Anexo II

- Gestión Residuos
- Química
- Alimentación
- Fabricación

Puedes consultar el listado completo en este documento de incibe_

3 - ¿Cómo me afecta?

Medidas concretas definidas en NIS2

El Artículo 21 de la DIRECTIVA (UE) 2022/25555 de 14 de diciembre de 2022 establece el conjunto mínimo de medidas de ciberseguridad que las organizaciones deben implementar. No se trata de controles genéricos: la directiva exige medidas "adecuadas y proporcionadas" al riesgo, lo que en entornos industriales implica adaptarlas a la realidad de los sistemas OT, tecnología obsoleta, procesos continuos y arquitecturas mixtas.

Gestión de riesgos

Identificar activos críticos (líneas, PLCs, equipos de red, servidores SCADA, software de supervisión e ingeniería, etc.), evaluar vulnerabilidades y documentar riesgos operacionales.

Gestión de incidentes

Capacidad real para detectar, analizar y responder a incidentes. Incluye procedimientos OT específicos, notificaciones obligatorias y coordinación con IT.

Continuidad y recuperación

Generar planes y estrategias que garanticen que la producción puede mantenerse o recuperarse con rapidez tras un incidente, desde redundancias hasta restauración segura de configuraciones de PLCs.

Cadena de suministro

Evaluación de proveedores, integradores, mantenedores y fabricantes.
Exigir requisitos de ciberseguridad a tu cadena de suministro e incluir requisitos mínimos de ciberseguridad en contratos.

Seguridad de red y sistemas

Segmentación de redes, implementación de firewalls industriales, análisis de protocolos, control de acceso a dispositivos críticos, gestión de configuraciones y bastionado de PLCs y HMI.

Gestión de vulnerabilidades

Generar un inventario detallado de todos los activos, realizar evaluación continua de vulnerabilidades para corregir o aplicar mitigaciones cuando no es posible parchear.

Pruebas, auditorías y monitorización

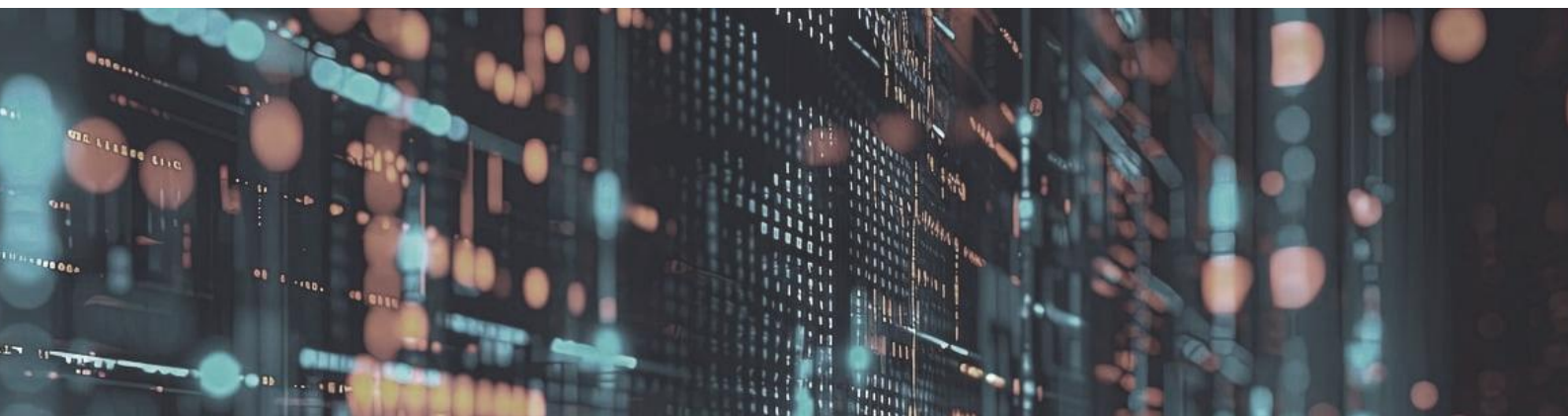
Revisiones periódicas de la instalación, herramientas de monitorización (IDS/OT) y auditorías regulares para demostrar cumplimiento ante autoridades.

Conocimiento y formación

Realizar programas formativos específicos para operadores, mantenimiento, ingeniería y dirección, orientados a riesgos reales de OT.

Gobernanza y responsabilidad

Implicación de la alta dirección, roles claros en OT/IT y trazabilidad documental de las decisiones.



4 - ¿Por dónde empezar?

Saber qué medidas requiere NIS2 no basta: es necesario plantear un **enfoque estructurado y progresivo** para poder implementarlas en una planta industrial sin interrumpir la operación. El objetivo es transformar las obligaciones de la directiva en **acciones concretas y priorizadas**, adaptadas a la criticidad de los activos OT y a la capacidad de la organización.

1 Diagnóstico Inicial: ¿En qué punto estoy?

Entender el estado actual de la organización frente a NIS2

Inventario completo de activos OT y sistemas IT críticos.
Evaluación preliminar de riesgos, brechas y controles existentes
Identificación de *Quick Wins* y vulnerabilidades críticas de **fácil implementación y alto impacto**

2 Análisis de Riesgos

Identificar, evaluar y priorizar los riesgos que amenazan los activos críticos de la organización

Enumerar amenazas relevantes para tu sector.
Evaluación de impacto: Si se materializa el riesgo, ¿cuál es el daño? (financiero, operacional, reputacional)
Clasificar riesgos por probabilidad e impacto.
Priorización: ranking de riesgos que requieren atención inmediata.

3 Políticas y Procedimientos

Definir cómo se van a abordar las necesidades en ciberseguridad como organización

Definir principios vinculantes (políticas) y pasos operacionales (procedimientos) que estandaricen cómo la organización gestiona seguridad en acceso, cambios, incidentes y proveedores.

4 Controles Técnicos

Definir e implementar las medidas técnicas específicas

Implementación progresiva por fases, priorizando sistemas críticos, medidas de alto retorno y adaptándose al plan de inversión.

5 Validación y Auditoría periódica

Verificar que los controles implementados funcionan y mantienen cumplimiento

Las auditorías deben realizarse al menos anualmente y después de cambios significativos en sistemas críticos. El objetivo es detectar deficiencias antes de que sean explotadas y demostrar a autoridades regulatorias un nivel de cumplimiento sostenido.

La ciberseguridad es un viaje, no un destino. En EOHM acompañamos a organizaciones y empresas del sector industrial a través de cada fase de su estrategia de ciberseguridad, desde la evaluación inicial hasta la validación final, asegurando que la seguridad se integra de forma natural en tu operación, fortaleciendo la confianza y aportando estabilidad sin generar fricciones.

¿Listo para empezar? Contacta con nosotros.

eohm@eohm.es

EOHM
Everything Engineering

www.eohm.es