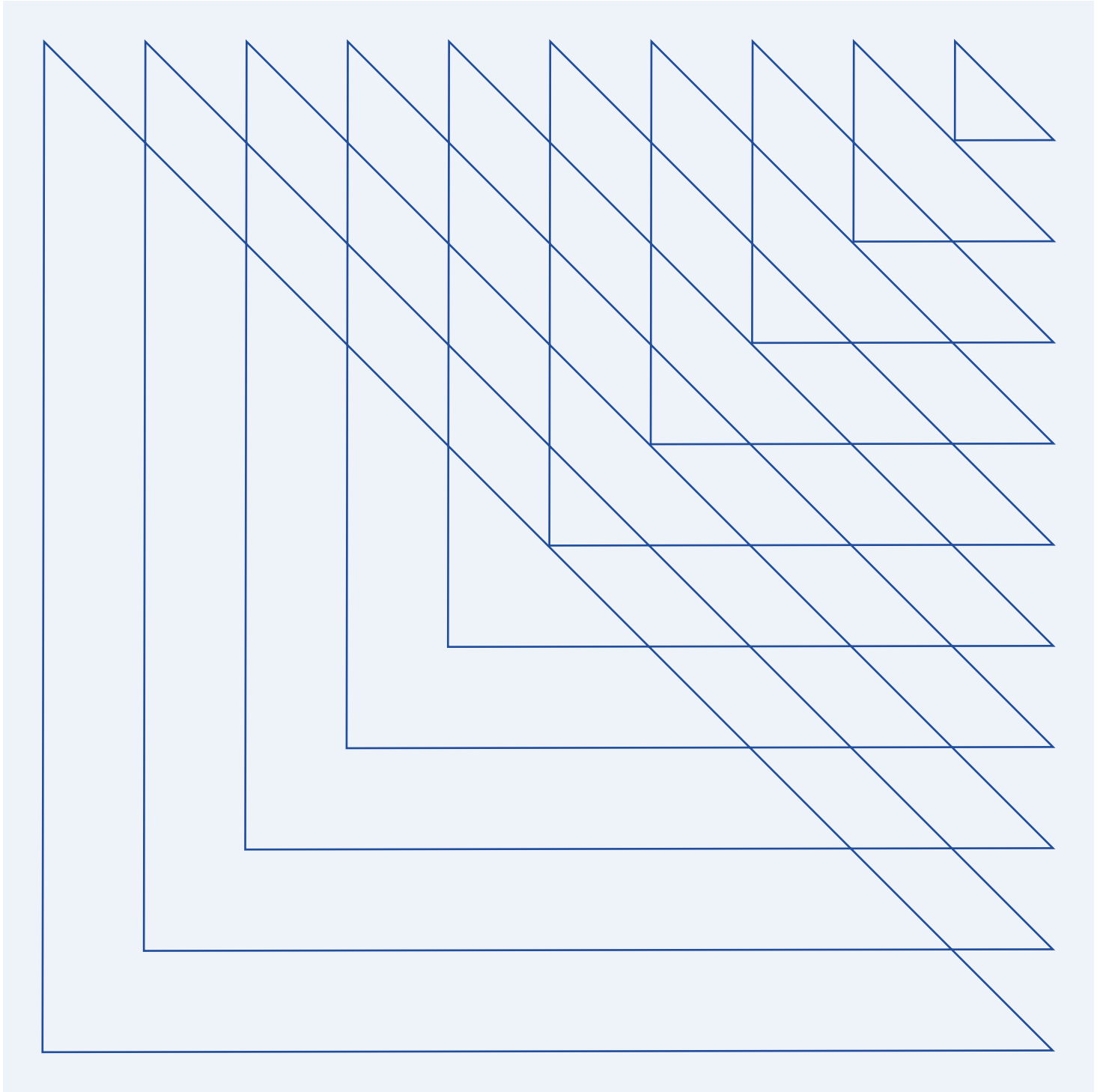
Whitepaper

GUÍA ACTUALIZADA PARA LA IMPLEMENTACIÓN EFECTIVA DE LA NORMATIVA

Directiva **NIS2**



ANTICIPANDO UN MUNDO CIBERSEGURO

S2GRUPO
Anticipando un mundo ciberseguro

Introducción

En 2016, la Unión Europea dio un paso histórico con la sanción de la **Directiva sobre redes y sistemas de información (NIS)**, la **primera legislación común en materia de ciberseguridad.** Su objetivo fue claro: mejorar la protección de los servicios esenciales para la sociedad y la economía frente a un entorno digital cada vez más expuesto a riesgos. Sin embargo, desde entonces, el **panorama ha cambiado**. Las amenazas se han vuelto más frecuentes, complejas y con un mayor impacto potencial.

En este contexto, la UE aprobó una actualización: la **Directiva NIS2**, que entró en vigor el 17 de octubre de 2024. Esta normativa **amplía de forma significativa su alcance, impone requisitos y obligaciones más estrictas y contempla sanciones más severas ante el incumplimiento**. Además, subraya la necesidad de una mayor cooperación entre Estados miembros para hacer frente a las amenazas.

Uno de los puntos clave de la NIS2 es que ya no afecta solo a sectores críticos como la energía o las telecomunicaciones, también alcanza a empresas medianas y grandes de sectores como el transporte, los servicios financieros, la gestión de residuos o la sanidad, entre muchos otros. Y un aspecto fundamental: si tu empresa es proveedor o subcontratista de una organización sujeta a la NIS2, también estás obligado a cumplir con ciertos estándares de ciberseguridad. La regulación pone el **foco en toda la cadena de suministro**, subiendo así el **nivel de exigencia y responsabilidad.**

En España, aunque ya se ha publicado el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, que dará respuesta a la trasposición de la Directiva, esta transposición aún no se ha completado, pero el reloj ya corre. Países como Italia, Bélgica, Grecia, Rumania, Hungría, Eslovaquia, Croacia, Letonia, Lituana, Finlandia o Dinamarca ya cuentan con legislación nacional. Esperar no es una opción: el cumplimiento de la NIS2 requiere una **planificación anticipada, inversión en capacidades y cambios organizativos** que no se resuelven de la noche a la mañana.

Desde S2GRUPO hemos actualizado el whitepaper que publicamos en 2025 para ayudarte a estar un paso adelante también este año. Aquí encontrarás los avances que ha habido en materia de NIS2 en los últimos meses, así como las claves que toda empresa debe conocer para **adaptarse a la nueva normativa, proteger su infraestructura digital y evitar sanciones** en un contexto donde la **ciberseguridad** ya no es solo un desafío técnico, sino una **responsabilidad estratégica**.

¿Cuál es la situación regulatoria actual de la Directiva europea NIS2 en España?

La Directiva (UE) 2022/2555, conocida como NIS2, estableció el 17 de octubre de 2024 como fecha límite para que los Estados miembros de la Unión Europea incorporaran sus requisitos a sus legislaciones nacionales.

En el caso de España, este proceso aún no se ha completado. El Gobierno aprobó el **Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad** en enero de 2025, que será el instrumento legal encargado de transponer la directiva al ordenamiento jurídico nacional. Sin embargo, la aprobación definitiva de la ley sigue pendiente.

Como consecuencia de este retraso, España recibió en mayo de 2025 un **dictamen motivado de la Comisión Europea**, el paso previo a posibles sanciones económicas ante el Tribunal de Justicia de la Unión Europea.

Este escenario podría interpretarse como un simple retraso legislativo. Sin embargo, la realidad es diferente: **la presión regulatoria ya está presente.**

Las autoridades nacionales, los reguladores sectoriales y las organizaciones afectadas están avanzando en la preparación para los requisitos de la directiva. La adaptación a NIS2 implica cambios que afectan a la gobernanza de la ciberseguridad, la gestión de riesgos, la resiliencia de las infraestructuras críticas y la responsabilidad de la alta dirección.

Además, organismos como el CCN-CERT han comenzado a publicar guías de apoyo para facilitar la adaptación de las organizaciones a los principios de la directiva, anticipando el marco que se aplicará cuando la legislación nacional quede definitivamente aprobada.

Actualmente, se espera que la **ley española de transposición de NIS2 sea aprobada durante el primer semestre de 2026**, estableciendo el régimen definitivo de supervisión y sanciones.

En este contexto, muchas organizaciones están adoptando un enfoque proactivo y comenzando a preparar su adecuación antes de la entrada en vigor formal del nuevo marco legal.

Comprender este momento regulatorio — caracterizado por retraso legislativo pero presión regulatoria activa— resulta clave para abordar desde ya la adaptación a NIS2 de forma eficaz.

¿Qué empresas deben cumplir con la **NIS2**?

La NIS2 aplica a todas las empresas medianas y grandes que operan en los sectores definidos por la directiva. Para determinar si tu empresa está sujeta, debes tener en cuenta, principalmente, dos criterios: el **sector de actividad** y el **tamaño de tu organización**.

Sector de actividad

Entidades esenciales

Grandes empresas que desempeñan un papel crucial en el desarrollo de actividades críticas y su interrupción puede tener un impacto significativo en la sociedad:

Energía
(electricidad, gas, petróleo, hidrógeno)

Transporte
(aéreo, ferroviario, marítimo y por carretera)

Banca y servicios financieros

Salud
(hospitales, clínicas, laboratorios)

Agua potable y aguas residuales

Infraestructura digital y gestión de servicios TIC
(DNS, CDNs, centros de datos, servicios gestionados, etc.)

Administración pública

Espacio

Entidades importantes

Entidades incluidas en el grupo anterior que no superen los límites de las medianas empresas, o que pertenezcan a otros sectores relevantes para la economía y la sociedad, como:

Fabricación, producción y distribución de químicos

Servicios postales y de mensajería

Proveedores de servicios digitales
(motores de búsqueda, redes sociales, etc.)

Alimentos
(producción, transformación y distribución)

Fabricación de productos
(sanitarios, electrónicos, eléctricos, maquinaria, vehículos, etc.)

Residuos y gestión de residuos

Investigación

Tamaño de la empresa

Los umbrales son:

Empresas medianas

- Más de **50 empleados**, o facturación anual superior a **10 millones** de euros.

Empresas grandes

- Más de **250 empleados** o facturación anual superior a **50 millones** de euros y balance general superior a 43 millones de euros.

GRUPOS DE EMPRESAS

Cuando una empresa supera los umbrales establecidos para ser considerada mediana o grande —ya sea por cantidad de empleados, facturación anual o balance general—, es posible que todo el grupo empresarial, incluidas sus filiales más pequeñas, quede sujeto a las obligaciones de la NIS2.

IMPORTANTE

Si bien las pequeñas empresas están en principio excluidas, **pueden quedar incluidas si su actividad tiene un impacto crítico**, por ejemplo, si son proveedores clave para empresas esenciales.

Requisitos más importantes de la **NIS2**

Gobernanza y responsabilidad

Los órganos de dirección deben aprobar y supervisar la implementación de las medidas de gestión de riesgos de ciberseguridad y pueden ser considerados responsables ante posibles infracciones. Para tener la capacidad de tomar decisiones en este ámbito de manera fundada, deben recibir formación en la materia.

Gestión de riesgos

Se deben aplicar las medidas técnicas, operativas y organizativas necesarias para gestionar los riesgos de ciberseguridad, a través del establecimiento de una política de seguridad, mecanismos para la gestión de incidentes, continuidad de negocio, monitorización de los sistemas de información y seguridad en la cadena de suministro, entre otros. Además, se debe evaluar de manera periódica la eficacia de estas medidas.

Cadena de suministro

Se debe evaluar y gestionar los riesgos derivados de proveedores o prestadores de servicios, especialmente si éstos prestan un servicio crítico a la organización.

Concienciación

Se deben establecer prácticas de ciberhigiene y llevar a cabo acciones de formación y concienciación en ciberseguridad para los empleados.

Control de acceso y gestión de activos

Se deben definir políticas de control de acceso y gestión de los activos, que establezcan mecanismos de autenticación multifactor, y el uso de criptografía y cifrado cuando sea necesario.

Notificación de incidentes

Se deben reportar los incidentes de seguridad a las autoridades competentes en los plazos establecidos:

- Alerta temprana: dentro de las 24 horas
- Notificación completa: en un máximo de 72 horas
- Informe final: en un plazo de un mes

Visión Integral de S2GRUPO: Alcance IT y OT

La Directiva NIS2 amplía el foco hacia las entidades esenciales e importantes, poniendo el acento en la protección de la organización y de las infraestructuras que sostienen servicios críticos para la sociedad. En la práctica, una parte muy significativa de esos servicios se presta sobre entornos operacionales y sistemas industriales, por lo que el componente OT resulta determinante en sectores como energía, agua, transporte, alimentación o la fabricación de dispositivos.

En este contexto, la gestión de riesgos de ciberseguridad no puede plantearse como un ejercicio limitado al ámbito IT. Los riesgos que NIS2 exige gestionar impactan de forma directa en los sistemas OT y en la continuidad operativa, y la directiva no establece una separación entre tipologías de sistemas: lo relevante es que el servicio esencial se mantenga y sea resiliente ante incidentes.

Sin embargo, el enfoque regulatorio y de cumplimiento se ha apoyado históricamente en marcos y certificaciones con una orientación marcadamente IT, que además permiten acotar el alcance y certificar sólo partes del entorno. Este planteamiento, aunque útil para estructurar gobierno y controles, no es suficiente cuando el objetivo es proteger infraestructuras híbridas y garantizar la continuidad de servicios soportados por sistemas industriales.

Por ello, S2GRUPO aporta una visión de cumplimiento basada en protección integral, extendiendo el alcance al mundo OT e integrando de forma coherente ambos dominios. El resultado es un enfoque IT+OT orientado a gestionar el riesgo de manera realista, reforzar capacidades de protección, detección y respuesta, y sostener la resiliencia operacional que NIS2 exige.

Problemáticas y Retos:

La ampliación del alcance de ciberseguridad al ámbito OT no es un simple ejercicio de extensión del perímetro. El reto principal reside en la **complejidad inherente de los sistemas industriales**, donde conviven tecnologías heterogéneas, ciclos de vida largos y condicionantes operativos que limitan la aplicación directa de enfoques habituales de seguridad IT.

Además, los entornos industriales han arrastrado durante años **riesgos estructurales** derivados de sistemas heredados, arquitecturas y protocolos específicos, y aproximaciones basadas en seguridad por oscuridad. Todo ello genera una superficie de exposición difícil de gobernar si no se entiende cómo se presta el servicio y qué dependencias lo sostienen.

Al mismo tiempo, el ecosistema industrial está evolucionando y, en muchos casos, incorporando capacidades que permiten elevar el nivel de ciberseguridad: se observa una adopción creciente de **protocolos con foco en la seguridad, PLCs con funciones de seguridad integradas, arquitecturas de referencia promovidas por fabricantes y mejoras tecnológicas orientadas a la segmentación de redes industriales**. Este avance es una oportunidad, pero también introduce nuevas dependencias tecnológicas que deben gestionarse con criterios de riesgo y continuidad.

Ante este escenario, es imprescindible contar con un **sistema de gestión** que asegure una gestión adecuada de los riesgos y que permita evaluar la eficiencia y eficacia de los controles desplegados. Sin embargo, conviene ser rigurosos con el alcance: marcos como **ISO 27001** o el **ENS** aportan estructura y buenas prácticas, pero han sido definidos tradicionalmente desde un prisma IT, centrados en la protección de la información y priorizando la confidencialidad y la integridad en el entorno corporativo.

En organizaciones cuya prestación de servicios esenciales depende de infraestructuras industriales, ese enfoque parcial es insuficiente para responder a lo que persigue NIS2. No se trata de "cumplir" por acumulación de evidencias, sino de **garantizar la continuidad de servicios esenciales para la sociedad**, y en este punto el componente industrial es determinante: más de un 60% de los sectores dentro del ámbito de aplicación de NIS2 presenta una fuerte componente OT.

Por tanto, no es suficiente mantener una aproximación clásica IT. La respuesta debe ser **integral, IT + OT**, y orientada a capacidades operativas y medibles.

Bajo esta visión, el foco de NIS2 debe materializarse en medidas que refuercen de forma coordinada:

- La protección de la infraestructura
- La gestión de ciberincidentes
- Las capacidades de monitorización de las infraestructuras IT+OT que dan soporte a los servicios esenciales
- La resiliencia operacional y la continuidad de negocio
- El aseguramiento de la cadena de suministro

Sanciones de la **NIS2**

Responsabilidad de la alta dirección

Durante mucho tiempo, la protección frente a amenazas digitales fue vista como una tarea exclusiva de los equipos de TI y los responsables técnicos. Sin embargo, la directiva NIS2 modifica este enfoque al asignar a la alta dirección la responsabilidad en casos de negligencia grave ante incidentes de ciberseguridad. Esta nueva perspectiva convierte a la ciberseguridad en un tema clave dentro de la estrategia organizacional.

En el caso de las entidades esenciales, esta exigencia va un paso más allá: impone una responsabilidad directa a los miembros de la junta y establece la necesidad de formación específica, cuando sea pertinente, para asegurar que cuenten con los conocimientos adecuados sobre las mejores prácticas en seguridad digital y puedan ejercer sus funciones de manera informada.

Multas financieras

La Directiva NIS2 diferencia claramente entre organizaciones esenciales e importantes a la hora de establecer sanciones económicas.

Para las entidades esenciales, los Estados miembros deben fijar un umbral mínimo de multa de 10 millones de euros o el 2 % de la facturación anual global, aplicándose el valor que resulte más alto.

En cambio, para las entidades importantes, se establecen sanciones de hasta 7 millones de euros o el 1,4 % de la facturación anual global, también eligiendo el mayor importe. Esta diferenciación refleja un modelo sancionador proporcional al nivel de criticidad de cada organización.

Sanciones no monetarias

Además de las posibles sanciones económicas, la Directiva NIS2 otorga a las autoridades nacionales competencias para aplicar medidas no monetarias. Entre estas se incluyen:

- Instrucciones vinculantes
- Órdenes para realizar auditorías de seguridad
- Requerimientos para notificar amenazas a los clientes
- Mandatos de cumplimiento específico

Si tu empresa está alcanzada por la NIS2, es fundamental tener en cuenta no solo las implicancias legales, sino también las consecuencias reputacionales de una brecha de seguridad grave. Un fallo en los controles o una respuesta inadecuada ante un ciberataque puede erosionar la confianza de clientes, socios e inversores.

Esta pérdida de credibilidad puede traducirse en una caída en las ventas, ruptura de alianzas estratégicas o pérdida de apoyo financiero. A su vez, el deterioro de la imagen corporativa puede dificultar la captación de talento cualificado, especialmente en áreas críticas como TI o ciberseguridad, ya que pocos profesionales querrán asociarse con una empresa que no prioriza la protección digital.

En este contexto, cumplir con NIS2 no es solo una obligación legal: es una condición para competir, proteger la reputación de la organización y garantizar su sostenibilidad en el tiempo.

¿Cómo implementar la Directiva **NIS2** en tu empresa?

Con la entrada en vigor de la directiva, miles de empresas que antes no estaban sujetas a obligaciones normativas ahora sí lo están, especialmente en sectores como el industrial, energético, sanitario o digital. La adecuación ya no es opcional: implica adoptar medidas concretas para proteger activos críticos, prevenir incidentes y coordinarse con las autoridades.

Para hacerlo de forma eficaz, es clave abordar el proceso con una visión estructurada. A continuación, compartimos cuatro pilares esenciales para implementar la normativa en tu organización.

01. Evalúa el punto de partida

Antes de implementar nuevas medidas, es fundamental conocer el estado actual de la ciberseguridad en la organización. Para ello, recomendamos realizar un *gap analysis* que permita detectar fortalezas, debilidades y riesgos no cubiertos, considerando de forma conjunta el entorno corporativo y el operacional.

Este diagnóstico debe incluir:

- Inventario de activos críticos (IT y OT).
- Evaluación de amenazas y vulnerabilidades.
- Revisión de políticas existentes y medidas técnicas ya implantadas.
- Grado de preparación para la detección y respuesta ante incidentes.

Para facilitar este proceso, es recomendable apoyarse en marcos de buenas prácticas alineados con el alcance. En el plano IT, ISO 27001 y NIST CSF, junto con el Esquema Nacional de Seguridad y guías prácticas de CCN-CERT o INCIBE, aportan estructura y criterios de evaluación. En paralelo, para el ámbito industrial, la serie IEC 62443 permite incorporar requisitos específicos de los sistemas de automatización y control, siendo especialmente relevante IEC 62443-2-1 como referencia para evaluar y orientar el programa de ciberseguridad en organizaciones propietarias de activos OT.

Al finalizar, se obtiene una visión clara y priorizada de qué debe mejorarse y con qué urgencia, con un enfoque coherente con una protección integral IT+OT.

02. Diseña tu hoja de ruta

Adecuarse a la Directiva NIS2 requiere estructura, foco y una hoja de ruta adaptada a cada organización. El primer paso es identificar las **acciones críticas** que deben abordarse con urgencia según el nivel de riesgo y la capacidad interna de ejecución.

Algunas de las medidas más prioritarias suelen ser:

- Definir una política de seguridad de la información.
- Establecer un marco de gobernanza con roles definidos y respaldo de la Dirección. Implantar un proceso formal de gestión de riesgos de ciberseguridad.
- Desarrollar un procedimiento de gestión de ciberincidentes, asegurando su conocimiento por parte de los implicados y probando su idoneidad (por ejemplo, a través de ejercicios tipo *table-top*).
- Asegurar la continuidad del negocio ante situaciones de contingencia, definiendo una estrategia de continuidad, y contando con un plan de crisis y planes de recuperación que sean probados regularmente.
- Asegurar la segmentación de redes IT/OT, controlar los accesos a las mismas y monitorizar la infraestructura IT+OT.
- Evaluar y gestionar el riesgo en la cadena de suministro, incluyendo requisitos de seguridad en los contratos con terceros.

Estas y otras acciones deben organizarse en un plan de cumplimiento que incluya:

- Cronograma con hito.
- Responsables asignados por iniciativa.
- Presupuesto estimado y recursos necesarios.
- Integración con procesos existentes (por ejemplo, derivados del SGSI en base a ISO 27001, IEC 62443-2-1 o ENS).

Es fundamental **documentar cada avance**: la trazabilidad será clave para auditorías, supervisiones o posibles exigencias legales.

Además, siempre deberás considerar las particularidades de tu sector. En entornos industriales, conviene centrar el esfuerzo en la protección del entorno operacional y sus dependencias, incluyendo redes industriales, sistemas de control y accesos de terceros. Esto exige una coordinación efectiva entre equipos IT y OT para que las decisiones de seguridad no comprometan la operación.

03. Adopta una cultura de la ciberseguridad

La Directiva NIS2 exige una cultura de seguridad transversal. Esto implica ir más allá de los controles técnicos o los procedimientos de actuación, asegurando que todas las personas entienden su rol en la protección de la organización.

En este sentido, asegúrate de que el plan de iniciativas comprenda:

- Ofrecer formación obligatoria en materia de ciberseguridad a los distintos niveles de la organización (Dirección, personal administrativo, personal técnico, etc.), y prácticas básicas de ciberhigiene (phishing, contraseñas, dispositivos externos, etc.).
- Realizar simulacros de incidentes adaptados al sector (por ejemplo, una intrusión en el entorno de producción).
- Implicar a mandos intermedios como agentes activos de la ciberseguridad.

Recuerda que, en sectores donde conviven perfiles técnicos y operativos, es esencial adaptar los contenidos a distintos niveles de responsabilidad y conocimiento.

04. Mantén las buenas prácticas y asegura el cumplimiento

Lograr la adecuación inicial a NIS2 es un hito, pero no el final del proceso. Dado el dinamismo de las ciberamenazas y la evolución normativa, la organización debe implementar un ciclo de mejora continua en su postura de seguridad.

Para ello, asegúrate de implementar buenas prácticas como:

Reevaluar periódicamente riesgos y controles: al menos una vez al año, revisar el análisis de riesgos y actualizarlo con nuevas amenazas, tecnologías o procesos.

Auditar y probar: combinar auditorías internas regulares con auditorías externas y pruebas de penetración anuales, tanto en redes IT como OT.

Monitorizar y aprender: mantener actualizadas las herramientas de detección, evaluar alertas y gestionar los incidentes.

Actualizar la documentación: adaptar el inventario de activos, los planes de respuesta, la normativa y procedimientos de seguridad y las evidencias de cumplimiento cada vez que cambie el entorno o la infraestructura.

Estar al día: seguir la evolución regulatoria, nuevas guías de ENISA y actualizaciones técnicas de INCIBE o CCN-CERT.

Involucrar a la dirección: informar regularmente al comité ejecutivo sobre el estado de la ciberseguridad y asegurar presupuesto y seguimiento.

La adecuación a NIS2 no es una lista de tareas aisladas, sino una estrategia a largo plazo para proteger el negocio.

Especialmente en sectores donde una interrupción puede afectar la producción, la reputación o la cadena de suministro completa, mantener un cumplimiento activo es sinónimo de resiliencia.

¿Por qué S2GRUPO?

S2GRUPO es una compañía europea especializada exclusivamente en ciberseguridad, ciberdefensa y ciberinteligencia, con una propuesta orientada a proteger infraestructuras críticas y sectores estratégicos desde una perspectiva integral IT+OT. Esta especialización permite abordar proyectos en los que el cumplimiento normativo debe traducirse en capacidades reales de protección, detección, respuesta y recuperación, especialmente cuando el servicio esencial depende de entornos industriales.

El valor diferencial se sustenta en una combinación de experiencia y capacidades propias que cubren todo el ciclo de vida de la ciberseguridad.

- Máxima solvencia en despliegue de SGSI (ISO 27001/ENS)
- Expertos en ciberseguridad industrial
- Enfoque integral IT+OT
- Capacidades propias de ciberdefensa (SOC)
- Expertos en gestión de crisis y gestión de incidentes

Por qué aproximar IT+OT de manera conjunta:

La convergencia entre IT y OT ha reducido la validez de enfoques basados en ámbitos aislados. En la práctica, las dependencias y flujos de información hacen que una aproximación exclusivamente IT o exclusivamente OT resulte limitada y, con frecuencia, ineficaz para proteger las operaciones. Por ello, el enfoque debe ser conjunto, consciente de las particularidades de cada entorno y orientado a gestionar riesgos de forma coordinada, integrando el conocimiento específico de cada dominio dentro de una estrategia común.

Nuestra Propuesta

Nuestra propuesta no se centra en “cumplir por cumplir”. Se orienta a realizar una gestión de riesgos de ciberseguridad real, desde una perspectiva de protección integral y con foco en incrementar el nivel de madurez como vía para sostener el cumplimiento y la continuidad del servicio. Este enfoque asume que, ante un incidente, no basta con disponer de evidencias documentales: es necesario demostrar que el riesgo se gestiona de manera adecuada y que las capacidades operativas están implantadas y funcionan.

Para ello, se aplica un marco de evaluación propio con enfoque IT+OT, unificando buenas prácticas basadas en estándares de referencia como ISO 27001 y ENS en el ámbito de gestión, e IEC 62443 para incorporar los requisitos específicos del entorno industrial. Esta base permite priorizar iniciativas con criterio de riesgo y orientar el esfuerzo para hacer las cosas bien desde el inicio, alineando el proyecto con el objetivo de NIS2.

¿Cómo podemos ayudarte?

La adecuación a NIS2 no es un ejercicio puntual, sino una transformación estructural que exige visión, especialización y continuidad. En S2GRUPO acompañamos a organizaciones públicas y privadas —especialmente en sectores críticos— en todo el ciclo de cumplimiento: desde el diagnóstico inicial hasta la implementación sostenida de medidas técnicas, organizativas y culturales.

Nuestro enfoque se basa en la realidad de cada organización: su sector, su nivel de madurez, sus riesgos y su cultura interna. No aplicamos recetas generales. Diseñamos soluciones a medida, respaldadas por equipos altamente especializados que combinan experiencia operativa, visión estratégica y conocimiento regulatorio.

01. Assessment de seguridad

Toda transformación efectiva comienza con un diagnóstico certero. En S2GRUPO realizamos un análisis integral del estado de cumplimiento frente a NIS2, identificando fortalezas, gaps y riesgos específicos en los entornos IT y OT. Lo hacemos combinando entrevistas con áreas clave, revisión documental, evaluación técnica y análisis contextual del sector. Esto nos permite ayudarte a tomar decisiones con datos objetivos y sin suposiciones.

02. Hoja de ruta

Una vez identificado el punto de partida, Aportamos nuestra amplia experiencia en el diseño de modelos de gobierno de seguridad, gestión de riesgos y cumplimiento normativo. Diseñamos junto a tu equipo una hoja de ruta adaptada a tus capacidades, prioridades operativas y presupuesto.

Esta planificación no sólo incluye los requisitos normativos, sino que los articula con los objetivos del negocio, asegurando que cada medida tenga impacto operativo y valor estratégico. La hoja de ruta incluye responsables, plazos, dependencias y mecanismos de control para facilitar la ejecución.

03. Implementación

No solo diseñamos, sino que ayudamos a ejecutar, fortalecer capacidades internas y demostrar cumplimiento ante auditorías. Contamos con equipos técnicos y funcionales que permiten llevar a cabo la adecuación de forma efectiva y sostenida:

Red Team

Simulamos ataques reales para poner a prueba la resiliencia de tus sistemas, tanto en entornos IT como OT. Nuestras auditorías avanzadas revelan vulnerabilidades ocultas y evalúan la efectividad de los controles existentes. Más allá del diagnóstico técnico, aportamos recomendaciones accionables para elevar tu capacidad de defensa en escenarios críticos.

SecOps

Nuestro equipo evalúa, implanta y refuerza la infraestructura de seguridad de forma integral. Te ayudamos a seleccionar las tecnologías más adecuadas para tu entorno y a configurarlas con criterios de robustez y sostenibilidad. Desde arquitecturas *zero-trust* hasta soluciones específicas para entornos industriales, nuestra intervención garantiza que la inversión en seguridad sea eficaz, escalable y alineada con tus riesgos reales.

Detección y respuesta

Operamos uno de los pocos SOC (Security Operations Center) en Europa que combina visibilidad en entornos IT y OT. Nuestra capacidad de detección temprana, análisis de amenazas y respuesta rápida permite a las organizaciones contener incidentes, minimizar impactos y proteger la continuidad operativa. Supervisamos infraestructuras híbridas con herramientas avanzadas y equipos humanos especializados 24/7.

Seguridad conductual

La cultura organizativa es el primer cortafuegos. Desde S2GRUPO analizamos los comportamientos, riesgos y dinámicas internas de cada área para diseñar programas de concienciación ajustados a la realidad de tu empresa. Vamos más allá de la sensibilización: trabajamos para transformar hábitos, generar cambios sostenibles y medirlos a través de KPIs observables. Nuestro objetivo es convertir al personal en un activo de defensa.

En S2GRUPO protegemos lo esencial: los sistemas, procesos y activos que garantizan la continuidad de sectores estratégicos y la estabilidad de nuestra sociedad.

Diseñamos e implantamos soluciones avanzadas que combinan tecnología propia, inteligencia aplicada y excelencia operativa. Nuestra capacidad para proteger de forma convergente entornos IT y OT nos permite ofrecer una solución eficaz, alineada con la arquitectura tecnológica y los riesgos específicos de cada sector.

Combinamos tecnología soberana, inteligencia aplicada y experiencia operativa para acompañar a las organizaciones que no pueden permitirse fallar. Nuestro compromiso es claro: construir modelos de ciberseguridad robustos, sostenibles y alineados con la complejidad de cada entorno.

Trabajamos bajo un modelo integral que cubre todo el ciclo de vida de la ciberseguridad: prevención, detección, respuesta, recuperación y análisis forense. Lo hacemos con un enfoque full-cycle, centrado en el cliente y orientado a reducir la exposición al riesgo, cumplir con los marcos regulatorios más exigentes y fortalecer la resiliencia organizativa frente a amenazas cada vez más sofisticadas.

Colaboramos con empresas e instituciones que lideran sectores clave, ayudándoles a anticipar amenazas, reforzar su resiliencia y operar con confianza, incluso bajo las condiciones más exigentes.

¿Quieres saber más?

Agenda una reunión 1:1 con nuestros expertos para discutir el informe, definir tus necesidades y prioridades de seguridad.

Contacta con nosotros

Tendencias en Ciberseguridad 2026

Un informe completo que ofrece una visión integral sobre el panorama de la ciberseguridad en los próximos meses.

Descarga el informe ›

Whitepaper Ciberseguridad OT y continuidad operativa

Presentamos un análisis del estado actual de la ciberseguridad en entornos industriales, proporcionando una visión estratégica y práctica que ayude a comprender su impacto y avanzar hacia un modelo de protección eficaz.

Descarga el informe ›

Reglamento DORA

Conoce cómo las entidades financieras y sus proveedores de servicios tecnológicos deberán implementar los requisitos técnicos establecidos por el reglamento.

Descarga el informe ›

Más allá de los algoritmos: los verdaderos riesgos de la IA

Analizamos en profundidad cómo los riesgos de la IA se manifiestan en tres niveles —técnico, operativo y humano—, qué actores los explotan y qué estrategias permiten mitigarlos. Una guía clara y práctica para CISOs que buscan anticiparse al nuevo panorama de amenazas y proteger la innovación sin frenar su potencial.

Descarga el informe ›

S2GRUPO

Anticipando un mundo ciberseguro

WWW.S2GRUPO.ES