semantic
systems

e-book
Tecnológico

La Directiva NIS2: ¿qué implica para las empresas en sectores críticos?

ÍNDICE

01 ¿Qué es la Directiva NIS2?

La Directiva NIS2 marca un nuevo estándar en ciberseguridad para la Unión Europea, con un enfoque en proteger infraestructuras críticas frente a crecientes amenazas digitales.

La Directiva NIS2 (Network and Information Security 2) es un documento que recoge la estrategia por medio de la cual la Unión Europea busca mejorar la seguridad cibernética de los estados miembros, con especial énfasis en la protección de las infraestructuras y servicios esenciales.

La directiva responde a la creciente necesidad de unificar y fortalecer la resiliencia de los sistemas digitales ante las amenazas cada vez más complejas y frecuentes en el ámbito de la ciberseguridad.

02 Principales objetivos de la Directiva NIS2

La Directiva NIS2 plantea tres objetivos clave que todas las empresas y organismos públicos deben considerar:

Armonización de medidas de seguridad: uno de los grandes retos de la ciberseguridad en la Unión Europea es la variabilidad de normativas, leyes y requisitos de un país a otro.

La Directiva intenta reducir estas diferencias estableciendo un marco común de seguridad que todos los estados deben seguir. Así, se espera facilitar la colaboración entre países, crear una respuesta unificada ante incidentes y mejorar la protección de las infraestructuras críticas.

Protección de los sectores económicos: la directiva se centra en los sectores que, debido a su criticidad o alta criticidad, son particularmente vulnerables a ciberataques.

Energía, transporte, banca, salud y telecomunicaciones, entre otros, son algunos de los sectores identificados como altamente críticos. Al proteger estos sectores, la directiva busca evitar las consecuencias devastadoras que podría tener un ataque cibernético en servicios clave para la sociedad.

Responsabilidad de la dirección y gestión de riesgos: la NIS2 no solo establece medidas técnicas, sino que también otorga un papel esencial a los órganos de dirección de las empresas en la gestión de la ciberseguridad.

Los altos directivos son ahora responsables de implementar medidas y estrategias de seguridad, así como de supervisar el cumplimiento normativo dentro de sus organizaciones.

03 Diferencias con la Directiva NIS1

La NIS2 surge como una actualización y ampliación de la anterior Directiva NIS, ya que esta última dejó áreas críticas sin cobertura suficiente. Las principales diferencias y mejoras de la NIS2 incluyen:

Alcance extendido: mientras que la NIS; ahora denominada NIS1 por la aparición de la 2, solo afectaba a algunos sectores estratégicos, la NIS2 incluye una mayor cantidad de sectores y tipos de empresas (entidades), garantizando que incluso organizaciones medianas y pequeñas en sectores estratégicos tomen medidas de protección.

Exigencia de cumplimiento y supervisión: la NIS1 había dejado a los Estados Miembros cierta flexibilidad en cuanto a la implementación y supervisión de las medidas.

La NIS2, en cambio, obliga a los países a garantizar un seguimiento y cumplimiento más riguroso, a través de la transposición en ley y estableciendo auditorías periódicas y sanciones específicas para aquellos que no cumplan con los requerimientos mínimos de seguridad establecidos en la directiva.

Aumento de las sanciones: a diferencia de la NIS1, la nueva directiva impone sanciones más estrictas y económicas que pueden suponer multas de hasta el 2% del volumen de negocio global de la empresa.

Esto busca incentivar a las empresas a invertir en medidas de ciberseguridad y a asumir una postura más proactiva en la prevención de riesgos e incidentes de ciberseguridad.

La Directiva NIS2 representa un cambio significativo en el enfoque de ciberseguridad de la Unión Europea, otorgando más responsabilidad a los líderes de las empresas y garantizando una respuesta unificada en toda la región.

04 Marco legislativo de la Directiva NIS2: adaptación y aplicación

La Directiva NIS2, oficialmente titulada como Directiva (UE) 2022/2555, fue aprobada por el Parlamento Europeo con el fin de establecer un nivel común de ciberseguridad en la Unión Europea.

Su naturaleza legislativa implica que todos los Estados Miembros deben trasponerla en sus legislaciones nacionales, adaptando sus normas internas para garantizar su aplicación efectiva en cada país.

Es importante señalar que **la NIS2 es una directiva**, lo que significa que establece objetivos y obligaciones comunes, pero permite a cada estado determinar cómo.

A diferencia de los reglamentos, que son aplicables directamente, las directivas requieren que los países elaboren sus propias leyes que incumplan con las metas establecidas a nivel europeo.

Esto otorga flexibilidad a cada Estado para ajustarse a sus contextos específicos, siempre que se mantengan los estándares establecidos por la Unión Europea.

La Directiva NIS2 establece plazos específicos para su transposición en la legislación nacional. Los Estados Miembros deben haber adaptado sus leyes para el 18 de octubre de 2024.

A partir de esta fecha, cada Estado miembro debe adoptar las medidas que garanticen el cumplimiento por parte de los sectores productivos llamados a ello y cuyas empresas estén catalogadas dentro de los requerimientos de la Directiva.

En el caso de España, la Directiva NIS2 será transpuesta a la legislación nacional mediante un **Real Decreto-ley,** que asegura la rápida adaptación de las directivas europeas a las leyes españolas. La fecha inicialmente acordada para finalizar la transposición y comunicar el Real Decreto-ley era 17 de octubre de 2024, sin embargo, dicha ley aún no ha sido comunicada.

Este Real Decreto-ley incluirá disposiciones específicas para adaptar los principios de la NIS2 a la normativa española y garantizará la Ciberseguridad para las entidades esenciales e importantes dentro de cada sector

El **Real Decreto 311/2022**, que regula el Esquema Nacional de Seguridad (ENS), también se verá impactado por esta adaptación. El ENS ya establecía medidas mínimas de seguridad para las entidades del sector público en España, y con la transposición de la NIS2 se ampliará su alcance para incluir sectores y entidades adicionales, especialmente aquellas clasificadas como esenciales bajo la nueva directiva europea.

05 Sectores críticos y de alta criticidad: ¿quién está afectado?

La Directiva NIS2 clasifica a ciertos sectores como “críticos” o de “alta criticidad” debido a su relevancia en la seguridad y estabilidad de la sociedad.

Estas clasificaciones determinan qué entidades deben cumplir con los requisitos más estrictos de ciberseguridad.

Los sectores incluidos en esta Directiva abarcan desde la energía hasta la banca, pasando por infraestructuras tecnológicas y el sector sanitario, todos ellos considerados vitales para el correcto funcionamiento de la sociedad.

06 Sectores de alta criticidad

La directiva especifica que ciertos sectores de actividad económica son de alta criticidad debido al impacto potencial de una interrupción en sus operaciones. Entre estos sectores se encuentran:

El sector de la energía, debido a que la generación y distribución de electricidad, gas y agua son fundamentales para la marcha de los estados. Un ciberataque a este sector podría causar un apagón generalizado o una interrupción de servicios básicos, con consecuencias graves para la seguridad pública.

Así mismo, **la banca e infraestructuras financieras** deben protegerse frente a ciberataques que puedan causar pérdidas financieras o filtrar datos sensibles de clientes. La protección de estos servicios es fundamental para la economía y la confianza de los usuarios.

Ni que decir tiene que **el sector sanitario** es también fundamental. Desde hospitales hasta proveedores de dispositivos médicos el sector salud es altamente crítico. Los ataques a infraestructuras sanitarias pueden poner en riesgo la vida de los pacientes y comprometer la privacidad de sus datos.

Por último, **las empresas de telecomunicaciones** juegan un papel crucial en la conectividad. Una amenaza a este sector podría derivar en interrupciones de las comunicaciones, afectando a servicios de emergencia y comunicaciones empresariales. Hoy en día se puede afirmar que un fallo a gran escala en las telecomunicaciones puede paralizar casi la totalidad de las operaciones y productividad de una nación.

07 Entidades esenciales e importantes

Además de los sectores críticos y de alta criticidad, la Directiva NIS2 identifica a las entidades en dos categorías según su importancia: **entidades esenciales y entidades importantes**. La clasificación de una entidad en una de estas categorías dependerá de su papel dentro del sector y del nivel de impacto que tendría una posible interrupción de sus servicios. Estos dos niveles de clasificación están diseñados para adaptar el grado de cumplimiento a la relevancia de la organización dentro de su sector.

Entidades esenciales: estas son organizaciones que, independientemente de su tamaño o volumen de negocios, cumplen una función crítica para la sociedad, como empresas que operan en energía, sanidad, banca, telecomunicaciones, confianza, transporte y otros sectores básicos suelen ser catalogadas como esenciales.

En caso de incumplimiento de la NIS2, las entidades esenciales se enfrentan a sanciones más elevadas debido a la relevancia de sus servicios.

Entidades importantes: aunque tienen un papel relevante, las entidades importantes pueden no tener un impacto tan crítico en la seguridad nacional como las entidades esenciales.

Sin embargo, estas entidades deben también implementar medidas de seguridad rigurosas y cumplir con las normativas de la NIS2, ya que un incidente de seguridad en sus operaciones podría afectar a otras entidades dentro del mismo sector, constituyéndose, así como un riesgo sistémico dentro de todo el entorno de la UE.

Proveedores y cadena de suministros la Directiva NIS2 establece claramente los requisitos para la gestión de la ciberseguridad en la cadena de suministros. Las entidades deben implementar medidas de efectividad para garantizar la seguridad en la cadena de suministros y mitigar los riesgos en contextos externos a las organizaciones.

La cadena de suministros se refiere a **todos los procesos de base tecnológica involucrados en la entrega de un producto o servicio, incluyendo proveedores y prestadores de servicios.**

08 ¿Qué implica estar en una de estas categorías?

Ser considerado como entidad esencial o importante tiene implicaciones directas para una empresa. Las organizaciones clasificadas en estas categorías están obligadas a cumplir con los requisitos de ciberseguridad establecidos en la directiva, que incluyen:

Evaluación de riesgos: las empresas deben realizar evaluaciones continuas de riesgos cibernéticos y actualizar su política de seguridad para adaptarse a las amenazas emergentes.

Supervisión y auditorías: las entidades esenciales y las importantes están sujetas a auditorías de seguridad, que pueden ser internas o externas, y deben presentar evidencia de cumplimiento ante las autoridades competentes.

Formación y concienciación: los altos directivos de estas empresas están obligados a asistir a programas de formación en ciberseguridad y deben asegurar que todos los empleados reciben capacitación adecuada para reducir los riesgos de ciberseguridad.

Sanciones por incumplimiento: tanto las entidades esenciales como las importantes pueden enfrentar sanciones si no cumplen con las normativas de la NIS2, aunque las penalizaciones son proporcionalmente más elevadas para las entidades esenciales debido a su mayor criticidad.

09 ¿Qué papel juega un SGSI en sus controles y procedimientos para el cumplimiento con la directiva?

La Directiva NIS2 lleva la ciberseguridad a un nuevo nivel de responsabilidad para las empresas, especialmente en la alta dirección. Aquí, no solo se pide que se implementen medidas técnicas y políticas, sino que también los líderes de las organizaciones se involucren activamente y supervisen que estas medidas funcionen en la práctica.

En el Artículo 20, la normativa recalca que **la alta dirección debe liderar la ciberseguridad**. Ya no es suficiente con delegar esta tarea a un departamento específico; los directivos son ahora responsables de asegurar que la empresa esté realmente protegida contra los riesgos cibernéticos.

De hecho, se espera que estén al tanto de cada paso en la gestión de estos riesgos, y que además rindan cuentas si algo falla. Es un cambio significativo, ya que convierte la ciberseguridad en un tema de gobernanza, poniéndola al mismo nivel de importancia que otras decisiones estratégicas.

Para facilitar esta transición, la directiva también insiste en que los altos cargos reciban **formación en ciberseguridad**. No se trata solo de aprender algunos conceptos, sino de entender a fondo cómo los riesgos cibernéticos pueden afectar a la operación de la empresa y cómo gestionarlos. Además, esta formación debe llegar a todos los empleados, de manera que cada persona en la organización esté preparada para detectar y responder a posibles amenazas.

En cuanto al Artículo 21, las empresas deben establecer una serie de **medidas prácticas para gestionar los riesgos.** Estas medidas cubren tanto aspectos técnicos como organizativos y buscan crear un entorno seguro y resiliente.

La idea es realizar un análisis de brechas (GAP Analysis) que permita ver hasta qué punto los procesos, el personal y los sistemas están alineados con los requisitos de ciberseguridad de la directiva.

Así, se pueden identificar áreas de mejora y asegurar que la organización tiene la madurez suficiente para enfrentar cualquier desafío digital.

Entre las medidas básicas, la directiva menciona la necesidad de tener una política de seguridad con un alcance definido, con roles y responsabilidades dentro del marco del gobierno de la seguridad, una clara gestión del riesgo y su correspondiente tratamiento y procedimientos establecidos para el control de acceso a sistemas críticos y la administración de privilegios

También se destacan los planes de continuidad de negocio (BCMP/BCP), los planes de respuesta a incidentes y la gestión de la cadena de suministro, asegurando que los proveedores también cumplen con los requisitos de ciberseguridad. Incluso se habla de controles específicos, como el doble factor de autenticación, la seguridad en correos electrónicos y la protección perimetral en redes.

Además, la NIS2 no se queda en la teoría: exige a las empresas evaluar continuamente si estas medidas están funcionando o no, mediante indicadores de rendimiento que midan su efectividad.

Y, si una organización descubre que no está cumpliendo con las medidas, debe corregir la situación de inmediato. Esta atención constante permite que la ciberseguridad no se vea como un proyecto de una sola vez, sino como un compromiso a largo plazo.

El A**rtículo 23 de la Directiva NIS2** establece obligaciones claras para las entidades en cuanto a notificaciones de incidentes de ciberseguridad, siendo el SGSI (Sistema de Gestión de Seguridad de la Información) una herramienta clave para cumplir con estos requerimientos.

Según la directiva, deben reportarse dos tipos de incidentes: aquellos que causan una perturbación grave en las operaciones de la entidad o tienen un impacto económico significativo, y aquellos que afectan material o inmaterialmente a terceros.

En caso de incidente, las empresas deben notificar al CSIRT de referencia en un plazo de 24 horas mediante una alerta temprana.

Esta debe actualizarse antes de las 72 horas, con una evaluación preliminar sobre su gravedad e impacto.

Para incidentes más complejos, puede ser necesario presentar un informe final detallado, hasta un mes después, incluyendo la descripción, las causas, y las medidas aplicadas. En casos transfronterizos, el CSIRT coordina la comunicación con otros países, garantizando una respuesta integral y rápida.

10 Soluciones de Semantic Systems para una Ciberseguridad Integral conforme a la NIS2

La Directiva NIS2 plantea un cambio significativo en los estándares de ciberseguridad de la Unión Europea, y su cumplimiento requiere una estrategia bien estructurada que aborde desde la gestión de riesgos hasta la capacitación del personal.

En este contexto, **Semantic Systems** ofrece un soporte integral para ayudar a las empresas a navegar con éxito estos nuevos requisitos de ciberseguridad, facilitando tanto la implementación de sistemas seguros como el fortalecimiento de la resiliencia organizativa.

Uno de los ejes centrales de este soporte es la **implantación de Sistemas de Gestión de Seguridad de la Información (SGSI) los cuales idealmente, deberían ser certificados. Dentro de los SGSI más reconocidos tenemos el estándar ISO27001:2022** y para España específicamente**, el Esquema Nacional de Seguridad (ENS), siendo este último de carácter obligatorio para entidades estatales o entidades las cuales tengan relaciones comerciales u operativas con el estado.**

Gracias a su plataforma ISMS, Semantic Systems ayuda a implantar y gestionar un SGSI en una organización como primer paso para conseguir una certificación de seguridad de la información. De esta forma, nuestros clientes podrán dar cumplimiento a los requisitos mínimo que en ciberseguridad requiere la Directiva NIS2

Además, para aquellas empresas que desean obtener certificaciones adicionales, el equipo de Semantic Systems ofrece un **acompañamiento consultivo**, orientado a alcanzar y mantener estándares internacionales en seguridad de la información y continuidad de negocio.

La capacidad de respuesta y adaptación de una organización es también fundamental para la NIS2. Con este objetivo, Semantic Systems ofrece servicios de auditoría interna de ciberseguridad, incluso con opciones avanzadas como el servicio vCISO (virtual Chief Information Security Officer), para proporcionar una visión profesional y externa sobre el estado de la seguridad de la empresa.

La capacidad de respuesta y adaptación de una organización es también fundamental para la NIS2. Con este objetivo, Semantic Systems ofrece servicios de **auditoría interna de ciberseguridad**, incluso con opciones avanzadas como el **servicio vCISO (virtual Chief Information Security Officer),** para proporcionar una visión profesional y externa sobre el estado de la seguridad de la empresa.

Este servicio puede complementarse con un **Plan director de Seguridad**, que ofrece un diagnóstico completo sobre el nivel de madurez en ciberseguridad y sugiere proyectos prioritarios para la mejora continua, identificando áreas de intervención específicas.

Además, la directiva hace hincapié en la concienciación y la capacitación del personal. Semantic Systems implementa **planes de concienciación y sensibilización en ciberseguridad**, que ayudan a formar a cada miembro de la organización en la identificación y respuesta a amenazas. Este “firewall humano” es crucial para el cumplimiento de la NIS2 y asegura que la seguridad no se limite a una serie de controles técnicos, sino que esté integrada en la cultura organizacional.

Por otro lado, Semantic Systems se especializa en el Análisis de Riesgos (AARR). Un AARR puede ejecutarse de forma independiente o como complemento de los productos y servicios de ciberseguridad, y permite identificar el nivel de exposición de los activos de información y así aplicar las medidas y contramedidas tendientes a clasificar y mitigar dichos riesgos.

Este servicio incluye desde el análisis de vulnerabilidades hasta test de intrusión, evaluando la capacidad de respuesta y detección frente a potenciales ataques y proporcionando una base sólida para el desarrollo de un **Plan de Respuesta a Incidentes.**

Así, las empresas pueden prepararse para responder eficazmente ante incidentes de ciberseguridad, cumpliendo con las normativas de la NIS2 y minimizando el impacto en su operación.

CONCLUSIÓN

En definitiva, Semantic Systems se posiciona como un **aliado estratégico en el camino hacia el cumplimiento de la NIS2**, ofreciendo no solo soluciones técnicas como la autenticación de doble factor (2MFA), la seguridad perimetral, copias de respaldo y la protección en correos electrónicos, sino también una estrategia de ciberseguridad integral que refuerza la resiliencia organizacional.

La combinación de consultoría, auditoría y formación permite a las empresas afrontar los desafíos de la NIS2 con la confianza de estar plenamente preparadas.

Semantic Systems

Creamos Tecnología, soluciones que digitalizan tus procesos

Semantic Systems es una compañía del sector TIC, proveedor global de soluciones tecnológicas que facilita y acompaña a las empresas en sus procesos de Transformación Digital, analizando, optimizando e implantado soluciones digitales en todos los procesos clave de su cadena de valor.

Contamos con amplia experiencia en proyectos, proporcionando soluciones en infraestructuras informáticas, outsourcing IT, desarrollo, implantación, integración y mantenimiento de software en empresas (ERP).

Fuertemente comprometidos con los desafíos de la industria 4.0, nuestros servicios ayudan a adaptar los procesos del negocio en el ámbito de los sistemas de información, telecomunicaciones y desarrollo de software.

CONSULTORÍA DIGITAL
Analizar, diseñar y desarrollar la estratega y el plan de digitalización

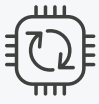
CLOUD COMPUTING
Servicio integral de infraestructuras con alto nivel de servicios gestionados y disponibilidad de sistemas

OUTSOURCING IT
Servicios personalizados de outsourcing global IT

COMUNICACIONES OT/IT Y CIBERSEGURIDAD
Diseño de arquitecturas de comunicaciones integrando soluciones de seguridad y conectividad OT/IT

ERP
Integración de todas las áreas del negocio con un software de gestión empresial SAP | INFOR | SAGE

INDUSTRIA 4.0
Soluciones globales en automatización y digitalización de procesos en empresas industriales adaptados a cada necesidad y sector



AUTOMATIZACIÓN DE PROCESOS
Soluciones digitales que automatizan todos los procesos clave de la cadena de valor de una empresa industrial

ANÁLISIS DE DATOS
Configuración e implementación de análisis y visualización de datos interactiva orientado a la toma de decisiones

Productos repcon

La Plataforma Tecnológica desarrollada por Semantic Systems permite representar conocimiento complejo en forma de red, ejecutar aplicaciones de misión crítica con alto rendimiento, manejar grandes volúmenes de datos aplicando reglas y construir herramientas de alta productividad en integración con los sistemas corporativos.

repcon pricing &quoting

Solución para la industrialización del proceso de generación de ofertas que permite crear propuestas 100% personalizadas, configurar soluciones complejas, administrar precios (en cascada…). Todo ello, integrable con el ERP/CRM, lo que resulta en una mejora sustancial de la productividad.

repcon configurator

Solución de configuración y personalización de productos con múltiples posibilidades y combinaciones, que automatiza los procesos desde el área comercial, hasta oficina técnica, administración de pedidos e ingeniería de fabricación, al determinar la estructura de materiales a fabricar y la ruta de fabricación.

repcon factory

Software para la captura de datos en planta de operarios y máquinas, el modelado, y la visualización de líneas de producción y máquinas en tiempo real. Automatización y control en planta dirigida a la gestión de la información del proceso productivo: órdenes de fabricación, personal, incidencias y alertas.

repcon dpa

Solución modular, para la digitalización y automatización de procesos administrativos, que se integra con los sistemas ERP/CRM y con todos los procesos relacionados con clientes y/o proveedores (de ofertas, pedidos, albaranes, facturas...)

repcon sii

Suministro inmediato de información. Solución que facilita el cambio del sistema de gestión actual del IVA, que pasa a un nuevo sistema de llevanza de los libros de registro del Impuesto sobre el Valor Añadido a través de la Sede Electrónica de la AEAT, mediante el suministro cuasi inmediato de los registros de facturación.

repcon TicketBai

Software que permite llevar a cabo un control de las actividades e ingresos económicos de las empresas, asegurando el cumplimiento de las obligaciones legales y técnicas que impone la normativa TicketBAI/Batuz.

semantic systems

94 454 55 50

www.semantic-systems.com

comercial@semantic-systems.com