UNIÓN EUROPEA

DIRECTIVA NIS2

(Directiva UE 2022/2555)

Medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión

Resumen en español para CISOs y responsables de cumplimiento

Referencia del documento

Campo	Valor
Nombre oficial	Directiva (UE) 2022/2555
Fecha de adopción	14 de diciembre de 2022
Fecha de publicación	27 de diciembre de 2022 (DO L 333/80)
Entrada en vigor	16 de enero de 2023
Plazo de transposición nacional	17 de octubre de 2024
Instrumento derogado	Directiva (UE) 2016/1148 (NIS1)

> Este documento es un resumen no oficial de la Directiva NIS2 de la UE de 14 de diciembre de 2022; no constituye una traducción con valor jurídico vinculante. Para una interpretación vinculante, consulte el texto oficial en DO L 333/80, 27.12.2022.

Índice

1. Resumen ejecutivo

La **Directiva NIS2** (Directiva UE 2022/2555), adoptada por el Parlamento Europeo y el Consejo el 14 de diciembre de 2022, es la directiva marco de ciberseguridad de la UE. Deroga y sustituye a la anterior Directiva NIS1 2016/1148 con efecto desde el 18 de octubre de 2024.

Las revisiones concluyeron que, si bien NIS1 contribuyó a elevar el nivel de ciberresiliencia en toda la Unión, resultó insuficiente para hacer frente a las amenazas de ciberseguridad actuales y futuras. NIS2 amplía sustancialmente el ámbito de aplicación, introduce criterios uniformes, refuerza las obligaciones de gestión de riesgos y notificación de incidentes, y establece disposiciones de ejecución con mayor efecto disuasorio.

Los cinco pilares de la Directiva

1. **Ámbito ampliado**: más sectores y empresas quedan sujetos a regulación.
2. **Gestión de riesgos reforzada**: 10 medidas técnicas y organizativas mínimas de obligado cumplimiento en virtud del artículo 21.
3. **Notificación de incidentes rápida y por fases**: alerta temprana en 24 horas, notificación del incidente en 72 horas, informe final en 1 mes.
4. **Responsabilidad del órgano de dirección**: la alta dirección puede incurrir en responsabilidad personal.
5. **Sanciones disuasorias**: multas administrativas de hasta el 2 % del volumen de negocio anual mundial o 10 millones de euros.

2. Objeto y base jurídica

La base jurídica de la Directiva es el **artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE)**, que autoriza medidas de aproximación de las normas nacionales con el fin de establecer y garantizar el funcionamiento del mercado interior.

Los principales objetivos de la Directiva son:

- Eliminar las grandes divergencias entre los Estados miembros y establecer normas mínimas comunes de ciberseguridad;
- Establecer mecanismos eficaces de cooperación transfronteriza e intercambio de información;
- Actualizar la lista de sectores y actividades sujetos a obligaciones de ciberseguridad para reflejar el panorama actual de amenazas;
- Proporcionar mecanismos de ejecución y recurso que garanticen el cumplimiento efectivo de las obligaciones;
- Reforzar las capacidades de ciberresiliencia de los operadores de infraestructuras críticas y los prestadores de servicios digitales.

La Directiva se aplica sin perjuicio y de conformidad con el Derecho de la UE en materia de protección de datos personales (RGPD, Reglamento UE 2016/679) y privacidad en las comunicaciones electrónicas (Directiva 2002/58/CE).

3. De NIS1 a NIS2: ¿por qué una nueva regulación?

NIS1, que entró en vigor en 2016, fue la primera regulación horizontal de ciberseguridad de la UE. El proceso de revisión reveló diferencias graves en la aplicación entre los Estados miembros, con la determinación del ámbito de aplicación dejada en gran medida a la discreción de cada Estado miembro, fragmentando así el mercado interior.

Deficiencias identificadas en NIS1

Área problemática	Situación en NIS1	Solución en NIS2
Determinación del ámbito	A discreción de los Estados miembros; variación significativa en la práctica.	Norma de «tamaño máximo» uniforme en toda la UE (medianas y grandes empresas).
Lista de sectores	Número limitado de sectores; parte significativa de la economía digital excluida.	Cobertura sectorial mucho más amplia; infraestructuras digitales, administración pública, espacio, etc., incluidos.
Notificación de incidentes	Única fase; plazos y contenido variaban entre los Estados miembros.	Notificación multifase: alerta temprana en 24 h + notificación en 72 h + informe final en 1 mes.
Gestión de riesgos	Lenguaje general; medidas mínimas específicas poco claras.	El artículo 21 enumera 10 categorías de medidas mínimas obligatorias.
Sanciones	Aplicadas a niveles muy diferentes entre los Estados miembros.	Multas máximas armonizadas a escala de la UE (10 M EUR / 2 % del volumen de negocio).
Responsabilidad de la alta dirección	Sin claridad.	El órgano de dirección es personalmente responsable del cumplimiento; formación obligatoria.

NIS2 no es una actualización de NIS1; es una sustitución diseñada para producir un **marco de ciberseguridad único, armonizado y ejecutable** en toda la Unión.

4. Ámbito de aplicación y exclusiones

La Directiva cubre principalmente a las entidades que operan en sectores del **Anexo I (alta criticidad)** o del **Anexo II (otra criticidad)** dentro de la UE y que cumplen la definición de al menos mediana empresa. Con arreglo al artículo 2 del Anexo de la Recomendación 2003/361/CE de la Comisión, una mediana empresa es aquella con menos de 250 empleados y un volumen de negocios anual no superior a 50 millones de euros (o cuyo balance total no exceda los 43 millones de euros). NIS2 captura a las entidades que alcanzan o superan el umbral de mediana empresa: el piso práctico para las entidades en el ámbito de aplicación es de 50 empleados o 10 millones de euros de volumen de negocios (el límite superior de la «pequeña empresa» con arreglo a la misma Recomendación).

Entidades cubiertas independientemente del tamaño

- Proveedores de redes públicas de comunicaciones electrónicas y proveedores de servicios de comunicaciones electrónicas disponibles para el público;
- Prestadores de servicios de confianza (en virtud del Reglamento eIDAS UE 910/2014);
- Registros de nombres de dominio de primer nivel (TLD) y proveedores de servicios de DNS;
- Entidades que sean el único proveedor de un servicio en un Estado miembro o cuya interrupción del servicio pueda afectar significativamente a la seguridad, la salud o la protección públicas;
- Todas las entidades de la Administración pública central (definidas a nivel nacional por los Estados miembros).

Áreas excluidas del ámbito de aplicación

Las entidades públicas cuyas actividades se lleven a cabo principalmente en los ámbitos de la **seguridad nacional, la seguridad pública, la defensa o la garantía del cumplimiento de la ley** (prevención, investigación, detección y enjuiciamiento de infracciones penales) quedan excluidas del ámbito de aplicación de la Directiva. Las representaciones diplomáticas y consulares de los Estados miembros en terceros países y los servicios de confianza utilizados en sistemas cerrados también quedan excluidos.

5. Definiciones clave

Algunos conceptos básicos deben comprenderse claramente para interpretar correctamente la Directiva.

Término	Definición
Sistemas de redes y de información	Redes de comunicaciones electrónicas, cualquier dispositivo o grupo de dispositivos que procesa datos digitales, y todos los datos digitales procesados para el funcionamiento, uso, protección y mantenimiento de dichos sistemas.
Ciberseguridad	Todas las actividades necesarias para proteger los sistemas de redes y de información, los usuarios y otras personas frente a las ciberamenazas.
Incidente	Acontecimiento que compromete la disponibilidad, autenticidad, integridad o confidencialidad de datos almacenados, transmitidos o procesados, o de los servicios ofrecidos a través de sistemas de redes y de información o accesibles mediante ellos.
Incidente significativo	Incidente que ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada, o que ha afectado o puede afectar a otras personas físicas o jurídicas causando perjuicios materiales o inmateriales considerables.
Ciberamenaza	Cualquier circunstancia, evento o acción potencial que pueda dañar, perturbar o afectar de forma adversa a los sistemas de redes y de información.
Ciberamenaza significativa	Una ciberamenaza que, en función de sus características técnicas, puede presumirse que tiene el potencial de causar un impacto grave en los sistemas de redes y de información de una entidad, en sus usuarios o en otras personas, causando perjuicios materiales o inmateriales considerables.
Vulnerabilidad	Debilidad, susceptibilidad o fallo de productos o servicios de TIC que puede ser explotado por una ciberamenaza.
Cuasiincidente	Acontecimiento que podría haber comprometido la disponibilidad, autenticidad, integridad o confidencialidad de datos almacenados, transmitidos o procesados, o de los servicios ofrecidos a través de sistemas de redes y de información, pero que se evitó con éxito antes de que se materializara.
CSIRT	Equipo de respuesta a incidentes de seguridad informática, equipo técnico responsable de la gestión de incidentes.
ENISA	Agencia de la Unión Europea para la Ciberseguridad; desempeña un papel central de asesoramiento y apoyo en la aplicación de la Directiva.

6. Categorías de entidades: esenciales e importantes

La Directiva divide todas las entidades en su ámbito de aplicación en dos categorías principales. Esta distinción determina cómo se aplican las obligaciones y el régimen de supervisión y garantía del cumplimiento.

Criterio	Entidades esenciales	Entidades importantes
Sector	Anexo I, sectores de alta criticidad	Anexo II, otros sectores críticos (y medianas empresas del Anexo I)
Tamaño	Grandes empresas (250 o más empleados o 50 o más millones de euros de volumen de negocios)	Medianas empresas (entre 50 y 249 empleados)
Régimen de supervisión	Supervisión tanto ex ante como ex post	Solo ex post, ante evidencias o reclamación
Multa administrativa máxima	10 millones de euros o el 2 % del volumen de negocio anual mundial (el importe que sea más elevado)	7 millones de euros o el 1,4 % del volumen de negocio anual mundial (el importe que sea más elevado)
Sanciones a la alta dirección	Puede aplicarse la prohibición temporal de ejercer funciones directivas	No se aplica la prohibición temporal de ejercer funciones directivas

> **Nota importante:** Si una entidad fue identificada como «operador de servicios esenciales» en virtud de NIS1, el Estado miembro puede decidir que dicha entidad sea directamente una entidad esencial en virtud de NIS2. Además, todas las entidades identificadas como «entidades críticas» en virtud de la Directiva 2022/2557 (CER) se consideran automáticamente entidades esenciales en virtud de NIS2.

7. Sectores en el ámbito de aplicación (Anexo I y Anexo II)

Anexo I, sectores de alta criticidad

Las grandes empresas en estos sectores son entidades esenciales; las medianas son entidades importantes.

Sector	Subsector / Tipo de entidad
Energía	Electricidad (generación, transporte, distribución, suministro); Calefacción y refrigeración urbanas; Petróleo (oleoductos, producción, almacenamiento, transporte); Gas natural; Producción, almacenamiento y transporte de hidrógeno
Transporte	Aéreo (compañías aéreas, aeropuertos, gestión del tráfico aéreo); Ferroviario (administradores de infraestructuras, operadores ferroviarios); Marítimo (operadores de transporte marítimo y de vías navegables interiores); Viario (sistemas de transporte inteligente, operadores viarios)
Banca	Entidades de crédito según el Reglamento (UE) 575/2013
Infraestructuras de los mercados financieros	Centros de negociación (bolsas) y contrapartes centrales (CCP)
Sanidad	Prestadores de asistencia sanitaria; laboratorios de referencia de la UE; entidades que realizan actividades de I+D de medicamentos; fabricantes de productos farmacéuticos; fabricantes de dispositivos médicos considerados críticos durante emergencias de salud pública (según el Reglamento (UE) 2022/123)
Agua potable	Proveedores y distribuidores de agua para consumo humano
Aguas residuales	Entidades que recogen, eliminan o tratan aguas residuales urbanas, domésticas o industriales
Infraestructuras digitales	Puntos de intercambio de internet (IXP); proveedores de servicios de DNS (excluido el DNS raíz); registros de nombres de dominio de primer nivel; proveedores de servicios de computación en nube; proveedores de servicios de centros de datos; proveedores de redes de distribución de contenidos (CDN); prestadores de servicios de confianza; proveedores de redes o servicios públicos de comunicaciones electrónicas
Gestión de servicios de TIC (B2B)	Proveedores de servicios gestionados (MSP); proveedores de servicios de seguridad gestionados (MSSP)
Administración pública	Entidades de la Administración pública central y regional según la definición de cada Estado miembro
Espacio	Operadores de infraestructuras terrestres cuya propiedad, gestión y explotación corresponden a los Estados miembros o a entidades privadas

Anexo II, otros sectores críticos

Sector	Subsector / Tipo de entidad
Servicios postales y de mensajería	Proveedores de servicios postales (incluidos los servicios de mensajería)
Gestión de residuos	Entidades que prestan servicios de recogida, reciclado y eliminación de residuos
Fabricación, producción y distribución de productos químicos	Entidades que se dedican a la fabricación, producción y distribución de sustancias químicas
Producción, transformación y distribución de alimentos	Grandes empresas que se dedican a la producción, transformación y distribución al por mayor de alimentos
Fabricación	Dispositivos médicos/dispositivos médicos para diagnóstico in vitro; productos informáticos, electrónicos y ópticos; material eléctrico; maquinaria y equipo n.c.o.p.; vehículos de motor, remolques y semirremolques; otro material de transporte
Proveedores digitales	Mercados en línea; motores de búsqueda en línea; plataformas de servicios de redes sociales
Investigación	Organismos de investigación que llevan a cabo investigaciones con fines comerciales

8. Obligaciones de los Estados miembros

La Directiva impone obligaciones tanto a los Estados miembros como a las entidades del sector privado. Cada Estado miembro debe adoptar las siguientes medidas:

Estrategia nacional de ciberseguridad. Adoptar una estrategia nacional de ciberseguridad con objetivos estratégicos claros, prioridades y un marco de gobernanza. La estrategia aborda cuestiones como la seguridad de la cadena de suministro, el ransomware, el apoyo a las pymes, el código abierto y la ciberdefensa activa.

Autoridad(es) competente(s). Designar o establecer una o varias autoridades competentes para garantizar la aplicación y supervisión de la Directiva.

Punto de contacto único (PCU). Designar un punto de contacto único responsable de la coordinación transfronteriza a escala de la UE.

CSIRT. Establecer o designar uno o varios CSIRT responsables de la gestión de incidentes, la supervisión proactiva, la divulgación coordinada de vulnerabilidades y la cooperación nacional e internacional.

Lista de entidades. Mantener, actualizar periódicamente y transmitir a la Comisión una lista de entidades esenciales e importantes y de entidades que prestan servicios de registro de nombres de dominio.

Divulgación coordinada de vulnerabilidades. Designar un CSIRT como coordinador; promover la claridad jurídica para los investigadores de vulnerabilidades.

Asistencia mutua. Prestar asistencia mutua a otros Estados miembros en la supervisión y la garantía del cumplimiento transfronterizos.

Apoyo a las pymes. Facilitar orientación, herramientas gratuitas y un punto de contacto nacional o regional para las pequeñas y microempresas.

9. Medidas para la gestión de riesgos de ciberseguridad (artículo 21)

La disposición técnica más importante de la Directiva es el artículo 21. En él se enumeran las medidas técnicas, operativas y organizativas mínimas que las entidades esenciales e importantes deben aplicar. El enfoque se basa en una **perspectiva «basada en todos los peligros»**: no solo se cubren los ciberataques, sino también amenazas como los daños físicos, los desastres naturales, los fallos de equipos y los errores humanos.

Artículo 21, diez medidas mínimas

N.º	Medida	Descripción
1	Políticas de seguridad de los sistemas de información y análisis de riesgos	Análisis de todos los riesgos y elaboración por escrito de políticas generales de seguridad de la información.
2	Gestión de incidentes	Procesos de prevención, detección, respuesta y recuperación de incidentes.
3	Continuidad de las actividades	Gestión de copias de seguridad, recuperación en caso de catástrofe y gestión de crisis.
4	Seguridad de la cadena de suministro	Incluidas las prácticas de seguridad de los proveedores; cláusulas de ciberseguridad en los contratos con proveedores directos.
5	Seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información	Seguridad a lo largo del ciclo de vida, incluida la gestión y divulgación de vulnerabilidades.
6	Evaluación de la eficacia de las medidas	Evaluación periódica de la eficacia de las medidas para la gestión de riesgos de ciberseguridad.
7	Prácticas básicas de ciberhigiene y formación en ciberseguridad	Prácticas de ciberhigiene y formación de sensibilización para el personal.
8	Criptografía y cifrado	Políticas sobre el uso del cifrado; cifrado de extremo a extremo cuando proceda.
9	Seguridad de los recursos humanos, control de acceso y gestión de activos	Comprobaciones de seguridad del personal, autorización e inventario de activos.
10	Autenticación multifactorial y comunicaciones seguras	AMF cuando proceda, autenticación continua, comunicaciones de voz, vídeo y texto seguras, y sistemas de comunicaciones de emergencia seguros.

Estas medidas se aplican conforme al **principio de proporcionalidad**, teniendo en cuenta la exposición al riesgo de la entidad, su tamaño, su importancia sectorial y el posible

10. Obligaciones de notificación de incidentes (artículo 23)

La innovación operativa más importante de la Directiva es el régimen de notificación de incidentes en varias etapas. Las entidades esenciales o importantes deben notificar los **incidentes significativos**, definidos como aquellos que causan graves perturbaciones operativas, pérdidas económicas o un impacto sustancial en otras personas, al CSIRT o a la autoridad competente en los siguientes plazos.

Etapa	Plazo	Contenido
Alerta temprana	En el plazo de veinticuatro horas desde que se haya tenido constancia del incidente	Sospecha de que el incidente responde a una acción ilícita o malintencionada; posibilidad de repercusiones transfronterizas; información básica que permita al CSIRT tomar conocimiento.
Notificación del incidente	En el plazo de setenta y dos horas desde que se haya tenido constancia del incidente	Actualización de la alerta temprana; gravedad, impacto e indicadores de compromiso (IoC) cuando estén disponibles.
Informe intermedio/final	A más tardar un mes después de la notificación del incidente	Descripción detallada del incidente, su gravedad e impacto; tipo de amenaza explotada; medidas paliativas aplicadas y previstas; repercusiones transfronterizas, si las hubiere.
Informe de situación	Si el incidente sigue en curso en el momento de presentar el informe final	Informe de situación sobre el estado actual del incidente; informe final un mes después de concluida la gestión del incidente.

Notificación a los destinatarios del servicio: cuando sea probable que se produzca una ciberamenaza significativa, las entidades deberán notificar sin demora indebida y de forma gratuita a los destinatarios de sus servicios las posibles medidas paliativas y, cuando proceda, la propia amenaza, en un lenguaje claro y comprensible.

Cuasiincidentes y notificación voluntaria

Además de los incidentes, las entidades **pueden notificar voluntariamente cuasiincidentes y ciberamenazas significativas** al CSIRT o a la autoridad competente. Las entidades que no estén dentro del ámbito de aplicación de la Directiva también pueden notificar de forma voluntaria. La notificación voluntaria no impone obligaciones adicionales al notificante.

> **Impacto práctico:** La alerta temprana de 24 horas obliga a las entidades a tener un plan de respuesta a incidentes cibernéticos y un flujo de comunicación listos para activarse de inmediato cuando se detecte un incidente. Cumplir este plazo mediante procesos manuales y fragmentados resulta sumamente difícil.

11. Seguridad de la cadena de suministro

La mayoría de los grandes ciberataques de los últimos años alcanzaron a sus organizaciones objetivo a través de proveedores y suministradores de software, no mediante un ataque directo a la propia organización. La Directiva sitúa por tanto el riesgo de la cadena de suministro en el centro de las obligaciones de gestión de riesgos.

- Las entidades deben evaluar la **calidad, las prácticas de seguridad y los procedimientos de desarrollo seguro** de los productos y servicios de sus proveedores y prestadores de servicios.
- **Los requisitos de ciberseguridad deben incluirse en los contratos** con los proveedores directos.
- Debe ejercerse una diligencia especial al seleccionar **proveedores de servicios de seguridad gestionados (MSSP)**; estos proveedores son objetivos de alto valor para los atacantes.
- El Grupo de Cooperación, junto con la Comisión y la ENISA, lleva a cabo **evaluaciones coordinadas de los riesgos de seguridad** de las cadenas de suministro críticas (como se hizo para las redes 5G).
- Los **factores de riesgo no técnicos** también están dentro del ámbito de la evaluación, incluida la posible influencia indebida de terceros países sobre los proveedores, las vulnerabilidades o puertas traseras ocultas, y la dependencia del proveedor.

12. Responsabilidad del órgano de dirección

La Directiva garantiza que la ciberseguridad deje de ser un asunto confinado a los departamentos técnicos y pase a ser un **ámbito de responsabilidad directa de la alta dirección**. De conformidad con el artículo 20, los órganos de dirección de las entidades esenciales e importantes:

- Son responsables de **aprobar las medidas de gestión de riesgos** establecidas en el artículo 21 y de supervisar su aplicación;
- Pueden **incurrir en responsabilidad personal** por el incumplimiento de estas obligaciones;
- Deben recibir formación periódica en ciberseguridad para adquirir los conocimientos y competencias suficientes;
- Deben fomentar una formación similar entre su personal.

> **Importante:** En las entidades esenciales, la autoridad competente puede solicitar que se apliquen **prohibiciones temporales de ejercer funciones directivas** a la alta dirección (quienes ostenten la condición de consejero delegado o de representante legal). Se trata de una medida de último recurso, aplicable únicamente cuando se han agotado todas las demás opciones de ejecución.

13. Estructuras de cooperación a escala de la UE

La Directiva regula o refuerza diversas estructuras que garantizan una cooperación eficaz entre los Estados miembros:

Estructura	Función
Grupo de Cooperación	Apoya la cooperación a nivel estratégico; elabora programas de trabajo bienales; publica documentos de orientación; lleva a cabo evaluaciones coordinadas de riesgos para las cadenas de suministro críticas.
Red de CSIRT	Cooperación a nivel operativo; intercambio de información sobre incidentes; asistencia mutua; respuesta conjunta.
EU-CyCLONe	Red de organizaciones de enlace en materia de cibercrisis a escala europea; conecta los niveles técnico y político en incidentes y crisis a gran escala; elabora análisis de impacto.
ENISA	Establece y mantiene la base de datos europea de vulnerabilidades; presta apoyo técnico; elabora orientaciones; supervisa las políticas de ciberhigiene de los Estados miembros.
Mecanismos IPCR	Mecanismos de respuesta política integrada de la UE a crisis (Decisión de Ejecución del Consejo 2018/1993); gestión de crisis a escala de la Unión ante situaciones de emergencia a gran escala.
Coordinador de divulgación coordinada de vulnerabilidades de la red de CSIRT de la UE	Un CSIRT de cada Estado miembro es designado coordinador para gestionar la divulgación coordinada de vulnerabilidades transfronteriza.

Cooperación con terceros países: La UE puede celebrar acuerdos internacionales con terceros países u organizaciones internacionales en virtud del artículo 218 del TFUE. Tales acuerdos pueden, salvaguardando los intereses de la Unión y la protección de datos, permitir la participación de dichas partes en las actividades del Grupo de Cooperación, la Red de CSIRT o EU-CyCLONe.

14. Supervisión y garantía del cumplimiento

La Directiva establece diferentes regímenes de supervisión para las dos categorías de entidades. Las **entidades esenciales** están sujetas tanto a supervisión ex ante como ex post, mientras que las **entidades importantes** solo se supervisan ex post, ante evidencias o reclamación.

Facultades de supervisión de las autoridades competentes

- Llevar a cabo inspecciones in situ y supervisión a distancia;
- Solicitar auditorías de seguridad específicas (con posibilidad de que los costes corran a cargo de la entidad);
- Ordenar exploraciones de seguridad;
- Solicitar documentación sobre el cumplimiento de las medidas de gestión de riesgos;
- Solicitar información sobre actos de los que se sospeche que infringen la Directiva;
- Solicitar información que requiera acceso a datos personales y datos de tráfico cuando sea necesario.

Medidas de ejecución aplicables

- Emitir advertencias e instrucciones vinculantes;
- Ordenar la aplicación de medidas específicas o la subsanación de vulnerabilidades en un plazo determinado;
- Ordenar una auditoría independiente para verificar las medidas de gestión de riesgos;
- Ordenar a las entidades que informen a los destinatarios del servicio sobre la naturaleza del incumplimiento;
- Hacer declaraciones públicas (divulgando el nombre de la entidad y la naturaleza del incumplimiento);
- Para las entidades esenciales (último recurso): suspensión temporal de certificaciones o autorizaciones y prohibición temporal de ejercer funciones directivas a la alta dirección;
- Imponer o solicitar la imposición de multas administrativas.

15. Sanciones administrativas

La Directiva establece **umbrales máximos armonizados a escala de la UE** para las multas administrativas impuestas por los Estados miembros. Estos umbrales están vinculados al volumen de negocios mundial de la entidad, de forma similar al RGPD.

Tipo de entidad	Importe máximo (se aplica el que sea más elevado)
Entidades esenciales	10.000.000 EUR o el 2 % del volumen de negocio anual mundial
Entidades importantes	7.000.000 EUR o el 1,4 % del volumen de negocio anual mundial

Factores en la determinación de las multas

- Naturaleza, gravedad y duración de la infracción;
- Perjuicios materiales o inmateriales causados;
- Si la infracción fue intencional o negligente;
- Medidas adoptadas para prevenir o mitigar los daños;
- Grado de responsabilidad e infracciones anteriores;
- Grado de cooperación con la autoridad competente;
- Otros factores agravantes o atenuantes.

Las multas deben ser **proporcionadas**, y en su aplicación deben respetarse los derechos fundamentales, como el derecho de defensa, la presunción de inocencia y el derecho a la tutela judicial efectiva. Los Estados miembros también pueden establecer sanciones penales por las infracciones del Derecho nacional; no obstante, nadie puede ser sancionado dos veces por los mismos hechos en vulneración del principio **ne bis in idem**.

16. Calendario de aplicación y transición

Fecha	Acontecimiento
14 de diciembre de 2022	Adopción de la Directiva por el Parlamento Europeo y el Consejo
27 de diciembre de 2022	Publicación en el Diario Oficial de la UE (DO L 333/80)
16 de enero de 2023	Entrada en vigor de la Directiva (20 días después de la publicación)
17 de octubre de 2024	Plazo para que los Estados miembros transpongan la Directiva al Derecho nacional
18 de octubre de 2024	Comienzo de la aplicación de la Directiva
18 de octubre de 2024	Derogación de la Directiva (UE) 2016/1148 (NIS1)
17 de abril de 2025	Plazo para que los Estados miembros transmitan a la Comisión la lista de entidades esenciales e importantes
A partir del 17 de octubre de 2027	Revisión periódica de la aplicación de la Directiva por la Comisión (cada 36 meses)

Importante: NIS2 es una directiva; no se aplica directamente. Cada Estado miembro debe transponerla a su propio Derecho nacional. Por lo tanto, las obligaciones y sanciones concretas aplicables a una entidad dependen del acto nacional de transposición adoptado por el Estado miembro en el que opera.

17. Implicaciones para empresas no pertenecientes a la UE

Aunque NIS2 es una directiva de la UE, tiene implicaciones sustanciales para las empresas no pertenecientes a la UE, en particular las que prestan servicios al mercado europeo o suministran a entidades críticas con sede en la UE:

Empresas no pertenecientes a la UE directamente afectadas

- Los **proveedores de DNS, proveedores de servicios en la nube, operadores de centros de datos, proveedores de CDN, proveedores de servicios gestionados y de seguridad gestionados, mercados en línea, motores de búsqueda y plataformas de redes sociales** no pertenecientes a la UE que ofrezcan servicios en la UE deben designar un representante en la UE y cumplir las obligaciones de la Directiva;
- Las empresas no pertenecientes a la UE con filiales o sucursales en la UE pueden quedar sujetas a la Directiva a través de estas unidades;
- Los proveedores no pertenecientes a la UE que suministren productos o servicios a entidades esenciales o importantes de la UE estarán sujetos a **requisitos contractuales de seguridad de la cadena de suministro** impuestos por sus clientes (artículo 21(2)(d));
- Los MSP y MSSP no pertenecientes a la UE que presten servicios a infraestructuras digitales o entidades financieras de la UE pueden quedar directamente dentro del ámbito de aplicación.

Efectos indirectos

- Las evaluaciones de riesgo de la cadena de suministro realizadas por los clientes de la UE obligan a los proveedores no pertenecientes a la UE a elevar sus estándares de ciberseguridad;
- Las normas introducidas por la Directiva (ISO/IEC 27001, orientaciones de la ENISA, etc.) se están convirtiendo en **puntos de referencia de facto** en el mercado mundial;
- Las jurisdicciones ajenas a la UE utilizan cada vez más NIS2 como referencia al desarrollar su propia legislación en materia de ciberseguridad.

18. Hoja de ruta práctica de cumplimiento (10 pasos)

La siguiente hoja de ruta de 10 pasos sirve de guía práctica tanto para las empresas que operan en la UE como para aquellas que deseen alinearse voluntariamente con las normas NIS2.

Paso	Actividad
1. Determinación del ámbito	Determinar si la empresa opera en sectores del Anexo I o del Anexo II, si cumple los criterios de tamaño e identificar su categoría (esencial/importante).
2. Análisis de brechas	Evaluar el sistema de gestión de seguridad de la información existente frente a las 10 categorías de medidas del artículo 21; mapear las deficiencias.
3. Estructura de gobernanza	Establecer responsabilidades, líneas de reporte y procesos de aprobación a nivel de consejo / alta dirección; poner en marcha un programa de formación periódica.
4. Política y documentación	Elaborar o actualizar la política de seguridad de la información, la política de gestión de riesgos, la política de respuesta a incidentes, la política de uso aceptable y otros documentos.
5. Evaluación de riesgos	Realizar un inventario de activos, un análisis de amenazas y una evaluación de riesgos con enfoque de todos los peligros; establecer criterios de aceptación del riesgo.
6. Implantación de controles técnicos	Implantar AMF, cifrado, segmentación de red, arquitectura de confianza cero, gestión de registros, SIEM, EDR/XDR, copia de seguridad y soluciones de recuperación ante desastres.
7. Capacidad de respuesta a incidentes	Documentar el plan de respuesta a incidentes; asignar funciones y responsabilidades; establecer el flujo de comunicación para la alerta temprana de 24 horas; realizar ejercicios de simulación.
8. Gestión de la cadena de suministro	Inventariar proveedores; clasificarlos por nivel de riesgo; añadir cláusulas de ciberseguridad a las plantillas de contratos; realizar auditorías periódicas.
9. Formación y concienciación	Impartir formación anual de ciberhigiene a todo el personal; proporcionar formación especializada al órgano de dirección; realizar simulaciones de phishing.
10. Mejora continua	Realizar auditorías internas y externas; seguimiento de KPI; aprender de cada incidente; actualizar la evaluación de riesgos anualmente; obtener certificación (ISO/IEC 27001, certificación de ciberseguridad de la UE).

19. Conclusión y valoración

La Directiva NIS2 eleva sustancialmente el nivel de referencia de ciberseguridad de la Unión Europea. No se limita a imponer requisitos técnicos; también convierte la ciberseguridad en una **parte integral de la estructura de gobernanza y las operaciones empresariales de las organizaciones**.

Puntos fuertes de la Directiva

- **Amplio alcance**: aproximadamente 18 sectores y más de 100.000 entidades en el ámbito de aplicación en los 27 países de la UE;
- **Armonización**: condiciones de competencia equitativas en el mercado interior mediante criterios uniformes y un régimen de ejecución común en toda la UE;
- **Enfoque en la gobernanza**: al hacer responsable a la alta dirección, garantiza que la ciberseguridad impregne todos los niveles de la empresa;
- **Énfasis en la cadena de suministro**: responde a la realidad de que la mayoría de los ataques modernos llegan a través de la cadena de suministro;
- **Estructuras de cooperación**: coordinación multinivel a escala de la UE a través del Grupo de Cooperación, la Red de CSIRT y EU-CyCLONe.

Críticas y retos

- Retrasos y divergencias en la transposición de los Estados miembros; en la práctica, la aplicación uniforme en los 27 países de la UE es irregular;
- En particular para las medianas empresas, el coste del cumplimiento y cerrar la brecha de capacidad técnica plantean un reto serio;
- La aplicación del plazo de alerta temprana de 24 horas antes de alcanzar la madurez suficiente puede dar lugar a flujos de notificación superficiales o erróneos;
- Las áreas de solapamiento con las regulaciones sectoriales (DORA, en finanzas; eIDAS, en servicios de confianza; regulaciones sectoriales de aviación, etc.) pueden generar complejidad para las entidades.

Valoración global

NIS2 reencuadra la ciberseguridad, de ser una preocupación técnica, a convertirse en una cuestión de **continuidad del negocio, gobernanza corporativa y confianza de los clientes**. Para las entidades que operan en la UE o interactúan con ella, el cumplimiento es tanto una obligación legal como un medio para reforzar la resiliencia operativa.

Para las empresas no pertenecientes a la UE, NIS2 está estableciendo un nuevo **estándar de facto** de acceso al mercado de la UE y elevando las expectativas de ciberseguridad a escala mundial. El cumplimiento anticipado facilita el cumplimiento de las obligaciones contractuales y mejora la ciberresiliencia global.

> **Nota final:** Este documento resume las principales disposiciones de la Directiva para los lectores de habla hispana. Para los requisitos de cumplimiento específicos de su organización, consulte el texto oficial (DO L 333/80, 27.12.2022), el acto nacional de transposición de su Estado miembro y las regulaciones sectoriales; recurra a asesoramiento jurídico y de ciberseguridad cuando sea necesario.

Fuentes

- Directiva (UE) 2022/2555, número CELEX de EUR-Lex 32022L2555
- Diario Oficial de la UE L 333/80, 27 de diciembre de 2022
- ENISA, Agencia de la Unión Europea para la Ciberseguridad (www.enisa.europa.eu)
- Portal de Estrategia Digital de la Comisión Europea (digital-strategy.ec.europa.eu)

Más información sobre NIS2 de Rediacc

Este resumen describe la estructura y las obligaciones de la Directiva. Las guías complementarias de rediacc.com traducen esas obligaciones en decisiones operativas y de contratación concretas.

Tres guías complementarias

- **El artículo 21(2)(d) y el autoalojamiento.** Por qué el registro de TIC de terceros se reduce cuando el plano de datos nunca abandona su inquilinato. Para CISOs y responsables de contratación que renegocian DPA en 2026.
- **Eficacia continua sin teatro.** Los artículos 21(2)(e), (f) y 23 leídos conjuntamente. La bifurcación de tiempo constante que hace realistas los ejercicios semanales, y el calendario de notificación del artículo 23 que no se puede cumplir sin artefactos de calidad forense. Para responsables de SRE y operaciones.
- **El coste estructural del cumplimiento de NIS2.** La pila de cinco herramientas que las entidades esenciales del mercado medio están ensamblando en silencio, lo que un plano de control autoalojado colapsa, y las partidas que quedan en su lado de todos modos. Para CFO y compradores que se acercan a un ciclo de renovación.

Dónde encontrarlas

Las tres guías, junto con este resumen en formato PDF descargable, están disponibles en:

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ es una plataforma de infraestructura autoalojada registrada en Estonia (Código de registro 17363830, IVA EE102920091). El producto no es un sustituto de un programa de seguridad; es una capa de herramientas que elimina el riesgo de proveedor en el plano de datos que las herramientas tradicionales de copia de seguridad, recuperación ante desastres y datos de prueba no pueden eliminar. Nivel Community gratuito y niveles de pago desde 349 $/mes.

> Este documento y sus guías complementarias son material educativo. Las decisiones de cumplimiento específicas de su organización requieren asesoramiento jurídico y referencia al acto nacional de transposición en su jurisdicción.