

NORMA UE · CIBERSEGURIDAD

NIS2: la ciberseguridad que sus clientes de la UE le trasladan

NIS2 obliga a las empresas de la UE a revisar también la seguridad de sus proveedores. Por eso le llegan a usted cuestionarios, cláusulas de notificación y derechos de auditoría, aunque la ley ni siquiera lo mencione.

FUENTE LEGAL	VIGENTE DESDE	PLAZOS DE NOTIFICACIÓN	AFECTA A
Directiva (UE) 2022/2555	18/10/2024 (leyes nacionales)	24 h, 72 h, 1 mes	Proveedores de TI, software e industria

En pocas palabras

NIS2 es una directiva de la UE sobre ciberseguridad. Se aplica a entidades “esenciales” e “importantes” de 18 sectores, entre ellos energía, transporte, salud, infraestructura digital, gestión de servicios TIC, alimentos, química y la fabricación de ciertos bienes como maquinaria, vehículos o electrónica. Como es una directiva, cada Estado miembro dictó su propia ley. Las obligaciones básicas, sin embargo, son las mismas en todos lados.

Dos artículos le interesan a usted. El artículo 21 exige una gestión de riesgos de seguridad de la información, y dentro de ella incluye de forma expresa la seguridad de la cadena de suministro (apartado 2, letra d). La entidad tiene que tener en cuenta las vulnerabilidades de cada proveedor directo, la calidad de sus productos y sus prácticas de seguridad, incluido el desarrollo seguro (apartado 3). El artículo 23 regula la notificación de incidentes significativos a las autoridades: alerta temprana en 24 horas, notificación en 72 horas e informe final al mes.

Una empresa de la UE solo puede cumplir esos plazos si sus proveedores de servicios también avisan rápido. Por eso hoy figuran en muchos contratos de suministro, a menudo más estrictos.

A quién afecta en Sudamérica

A la mayoría de las empresas de la región NIS2 las alcanza de forma indirecta. Su cliente en Alemania, España o los Países Bajos está obligado y le traslada sus obligaciones por contrato. Casos típicos:

- Desarrollo nearshore desde Buenos Aires, Montevideo, Medellín o Lima que construye software para una distribuidora de energía o un hospital en la UE.

- Soporte de TI y centros de contacto con acceso a sistemas del cliente.
- Fabricantes de controladores, sensores o equipamiento industrial, por ejemplo de São Paulo o Córdoba, que abastecen a empresas de agua, fabricantes u operadores logísticos.
- Procesadores de alimentos cuyos compradores están alcanzados por NIS2 y por eso también preguntan por la seguridad informática de la producción.

Lo afecta directamente si ofrece ciertos servicios digitales en la UE: computación en la nube, centros de datos, redes de distribución de contenidos, servicios gestionados y servicios de seguridad gestionados, servicios DNS, registro de dominios, mercados en línea, motores de búsqueda y redes sociales. Para estos proveedores, según el artículo 26, es competente el Estado miembro del establecimiento principal. Quien no tiene establecimiento en la UE pero presta servicios allí debe designar un representante en la UE (art. 26, apartado 3). Si no lo hace, puede actuar cualquier Estado miembro en el que se presten los servicios (art. 26, apartado 4). Un proveedor de servicios gestionados de Porto Alegre con clientes en Portugal debería hacerlo revisar.

Aunque no tenga una obligación directa, conviene mirar la ley: casi todas las cláusulas que le presenta un cliente de la UE se pueden rastrear hasta el artículo 21 o el 23. Quien lo sabe negocia con más facilidad.

Plazos

Los Estados miembros debían trasponer NIS2 a más tardar el 17/10/2024, y las normas nacionales se aplican desde el 18/10/2024. Varios países llegaron tarde. En la práctica, hoy está resuelto en todos los mercados grandes y los departamentos de compras ya trabajan con los nuevos requisitos.

En enero de 2026 la Comisión propuso una modificación puntual de NIS2, junto con un nuevo marco jurídico para la seguridad de las cadenas de suministro TIC. Hasta que se apruebe, la directiva sigue rigiendo en su versión actual. Para los proveedores ya se ve venir que el tema de la cadena de suministro va a ganar peso. Quien empiece hoy no tendrá que rehacer casi nada después, porque las obligaciones de los artículos 21 y 23 ya rigen y son la base de cualquier pedido de un cliente. Los contratos marco que se renegocian con clientes de la UE ya traen esas cláusulas de todos modos.

NOTIFICACIÓN SEGÚN EL ART. 23	PLAZO PARA LA ENTIDAD DE LA UE	QUÉ SIGNIFICA PARA USTED
Alerta temprana	24 horas desde que toma conocimiento	Los clientes suelen exigir su aviso en pocas horas

NOTIFICACIÓN SEGÚN EL ART. 23	PLAZO PARA LA ENTIDAD DE LA UE	QUÉ SIGNIFICA PARA USTED
Notificación del incidente	72 horas	Primera evaluación, sistemas afectados, indicadores
Informe final	1 mes	Causa, medidas, efectos transfronterizos

Qué piden en concreto los clientes de la UE

Los requisitos se parecen mucho entre sí. Cuente con estos puntos:

- Un cuestionario de seguridad, a menudo basado en el anexo A de ISO/IEC 27001.
- Un certificado [ISO/IEC 27001](#) o, para proveedores SaaS con clientes en Estados Unidos, como alternativa un [informe SOC 2 tipo II](#).
- Cláusulas contractuales sobre la notificación de incidentes de seguridad, muchas veces en 24 horas o menos.
- Derechos de auditoría presencial o remota.
- Evidencia de gestión de vulnerabilidades y de pruebas de penetración.
- En software, una lista de componentes (SBOM) e información sobre desarrollo seguro.
- Un plan de contingencia y recuperación (continuidad del negocio).

Un certificado responde de una sola vez buena parte del cuestionario. Sin certificado, tiene que respaldar cada pregunta por separado, y con cada cliente de nuevo.

Cuide las contradicciones. Si en el cuestionario declara autenticación de dos factores para todas las cuentas y en la auditoría tiene que mostrar excepciones para sistemas heredados, pierde confianza. Es mejor una respuesta honesta con la fecha en que se cerrará la brecha. Guarde sus respuestas en un solo lugar, por ejemplo en una plataforma GRC como [Sightadel](#), para que ventas y TI den la misma información a cada cliente nuevo. En las licitaciones de grandes grupos europeos, la evaluación de seguridad suele decidir si usted queda siquiera entre los finalistas.

Primeros pasos

1. Aclare si presta en la UE alguno de los servicios que menciona el artículo 26. Si es así, necesita asesoramiento legal sobre el representante en la UE.
2. Haga una lista de sus clientes de la UE y de sus sectores. Un cliente de energía o de salud va a pedir más que un comercio.

3. Defina quién en la empresa evalúa los incidentes de seguridad e informa al cliente, con suplente y número de teléfono.
4. Revise sus sistemas más importantes desde afuera: ¿qué servidores, accesos y servicios se alcanzan desde internet? Herramientas como [veyrisk](#) lo muestran de forma continua.
5. Responda con honestidad un cuestionario real de un cliente y marque las brechas. De ahí sale su plan de acción.
6. Planifique a tiempo la certificación ISO/IEC 27001, porque montar el sistema de gestión y pasar la auditoría lleva su tiempo.

Cuánto camino ya recorrió se lo muestra en diez minutos el [diagnóstico UE](#) gratuito.

Relación con las certificaciones

NIS2 no exige ningún certificado. Pero los clientes de la UE aceptan pruebas reconocidas, porque con ellas documentan su propio deber de diligencia. [ISO/IEC 27001](#) cubre la mayoría de las preguntas, siempre que el organismo de certificación esté acreditado, en la región por ejemplo a través de la Cgcre en [Brasil](#), el OAA en [Argentina](#) o el ONAC en [Colombia](#). Los proveedores de la industria automotriz necesitan además [TISAX](#). Si trabaja para bancos o aseguradoras, se suma [DORA](#), y en productos conectados el [Reglamento de Ciberresiliencia](#).

También ayuda mirar el propio país. [Chile](#) tiene con la Ley Marco de Ciberseguridad una norma que se parece a NIS2 en muchos puntos; en [Uruguay](#) rigen obligaciones de notificación para sectores críticos. Quien ya está obligado allí tiene parte del trabajo hecho.

FAQ

¿NIS2 se aplica a mi empresa en Sudamérica?

De forma directa solo si ofrece en la UE ciertos servicios digitales como nube, centro de datos, servicios gestionados o DNS. En todos los demás casos, su cliente de la UE le traslada las obligaciones por contrato.

¿Necesito un certificado ISO 27001 para NIS2?

Por ley, no. Muchos clientes de la UE lo piden igual, porque les simplifica la revisión de la cadena de suministro que exige el artículo 21. Más información en la página sobre [ISO/IEC 27001](#).

¿Con qué rapidez tengo que notificar un incidente a mi cliente de la UE?

Lo dice su contrato. Como el cliente debe enviar una alerta temprana en 24 horas, muchos contratos exigen el aviso en pocas horas.

¿Qué es un representante en la UE?

Una persona o empresa establecida en la UE que actúa como interlocutor ante las autoridades para determinados proveedores de servicios digitales sin establecimiento en la UE (art. 26, apartado 3).

¿Qué herramientas ayudan con los requisitos NIS2 de un cliente?

[Sightadel](#) trae NIS2 e ISO/IEC 27001 como marcos y reúne políticas, riesgos, evidencias y respuestas a cuestionarios, con los datos alojados en Alemania. Para la evidencia de gestión de vulnerabilidades sirve un análisis externo continuo como [veyrisk](#); el [informe de ejemplo](#) muestra qué incluye.

Fuentes · Actualizado: 11 de octubre de 2026

Directiva (UE) 2022/2555 (NIS2), EUR-Lex: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

Comisión Europea: Directiva NIS2: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

ENISA: Directiva NIS2: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

Información general, no constituye asesoramiento legal. Prevalecen los textos oficiales.

PÓNGALO EN PRÁCTICA CON HERRAMIENTAS HECHAS EN ALEMANIA



Sightadel guía a su equipo por NIS2: plantillas, tareas, evidencias y preparación de auditorías en un solo lugar. Desarrollado y alojado en Alemania, con paquete de consultoría opcional.

[Ver Sightadel →](#)



veyrisk muestra lo que un atacante ve de su empresa desde fuera: servicios abiertos, certificados, vulnerabilidades conocidas. Puede presentar el informe a clientes europeos y auditores.

[Ver veyrisk →](#)



Valar es un firewall de hardware con software de neonotu. Protege oficinas y sedes y genera los registros que exigen NIS2 e ISO 27001.

[Ver Valar →](#)

Sightadel, veyrisk y Valar son productos de neonotu GmbH, empresa que opera MercoEU.

¿Qué parte de esto aplica a su empresa?

El diagnóstico UE gratuito se lo muestra en 10 minutos, según su sector y su país.

<https://www.mercoeu.com/es/diagnostico-ue>