Por qué el acceso remoto es el requisito más importante de NIS2

Por Netop | abril de 2026

Resumen ejecutivo

La Directiva NIS2 de la UE es la normativa de ciberseguridad más trascendental de la historia europea. Se aplica a aproximadamente 160.000 entidades de 18 sectores críticos, responsabiliza personalmente a la alta dirección en caso de incumplimiento e impone multas de hasta 10 millones de euros o el 2 % de la facturación anual global. Para los operadores de infraestructuras críticas, las organizaciones de defensa y los organismos gubernamentales, no se trata de un mero ejercicio de cumplimiento, sino de un cambio fundamental en la forma en que deben gestionarse las operaciones digitales.

De todos los requisitos que introduce la NIS2, el acceso remoto es donde más hay en juego. El acceso remoto se sitúa en la intersección de cinco obligaciones distintas de la NIS2 simultáneamente: seguridad de la cadena de suministro digital, control de acceso, cifrado, notificación de incidentes y certificación de ciberseguridad. Es el punto de entrada más explotado por los atacantes, el ámbito que con mayor frecuencia queda fuera del alcance de los marcos de seguridad heredados y el área con mayor concentración de riesgos de terceros. Una organización que cumpla todos los demás requisitos de la NIS2 pero no gestione adecuadamente el acceso remoto sigue estando peligrosamente expuesta, y afectada por varios artículos a la vez.

Este informe técnico explica por qué el acceso remoto exige una atención prioritaria en el marco de la NIS2, relaciona los requisitos de cumplimiento específicos con los controles operativos y muestra cómo el acceso remoto seguro de Netop permite a las organizaciones cumplir dichos requisitos. Netop aborda no solo lo que exige la NIS2, sino lo que los auditores necesitan ver: pruebas documentadas e inviolables de un acceso controlado, autenticado y supervisado a todos los puntos finales incluidos en el ámbito de aplicación.

El panorama normativo de la NIS2 en 2026

De la directiva a la aplicación

La NIS2, conocida oficialmente como Directiva (UE) 2022/2555, entró en vigor en enero de 2023. Se exigió a los Estados miembros que la incorporaran a sus legislaciones nacionales antes del 17 de octubre de 2024. Ese plazo se incumplió de forma generalizada: a principios de 2026, la transposición sigue en curso en toda la UE y los marcos de aplicación se están ultimando a nivel nacional.

Las organizaciones que consideraban el plazo de octubre de 2024 como un acontecimiento lejano se enfrentan ahora a un plazo de cumplimiento reducido, a medida que los reguladores nacionales activan sus poderes de supervisión y aplicación.

> **Situación normativa: marzo de 2026**
>
> *La transposición de la NIS2 se está acelerando en los Estados miembros de la UE tras el incumplimiento del plazo de octubre de 2024. Se están ultimando los marcos normativos nacionales y se espera que la actividad de aplicación aumente considerablemente a lo largo de 2026 y hasta 2027.*

Responsabilidad personal de la alta dirección

La NIS2 introduce un requisito que no existía en su predecesora: la responsabilidad personal de la alta dirección. En virtud del artículo 20, los órganos de dirección están obligados a aprobar medidas de gestión de riesgos de ciberseguridad y a supervisar su aplicación. El incumplimiento puede dar lugar a la suspensión de los ejecutivos, así como a multas contra la organización. La directiva eleva explícitamente la ciberseguridad al nivel del consejo de administración.

Para los CISO, CTO y CIO de las organizaciones reguladas por la NIS2, esto establece una responsabilidad personal directa de garantizar que sus controles de acceso remoto sean adecuados. El enfoque pasa de limitarse a contar con una política a demostrar (con evidencia) que dicha política se aplica de forma efectiva.

Ámbito de aplicación: quiénes están cubiertos

La NIS2 se aplica a entidades medianas y grandes de 18 sectores críticos e importantes: energía, transporte, banca, sanidad, infraestructura digital, gestión de servicios TIC, administración pública, espacio, fabricación, productos químicos, producción alimentaria, servicios postales, gestión de residuos, proveedores digitales y organizaciones de investigación.

La directiva también tiene alcance extraterritorial: las organizaciones no pertenecientes a la UE que presten servicios a entidades con sede en la UE o que operen en el mercado de la UE deben cumplirla. Para los contratistas de defensa globales, los operadores de infraestructuras multinacionales y los proveedores de tecnología internacionales con clientes de la UE, el cumplimiento de la NIS2 es obligatorio.

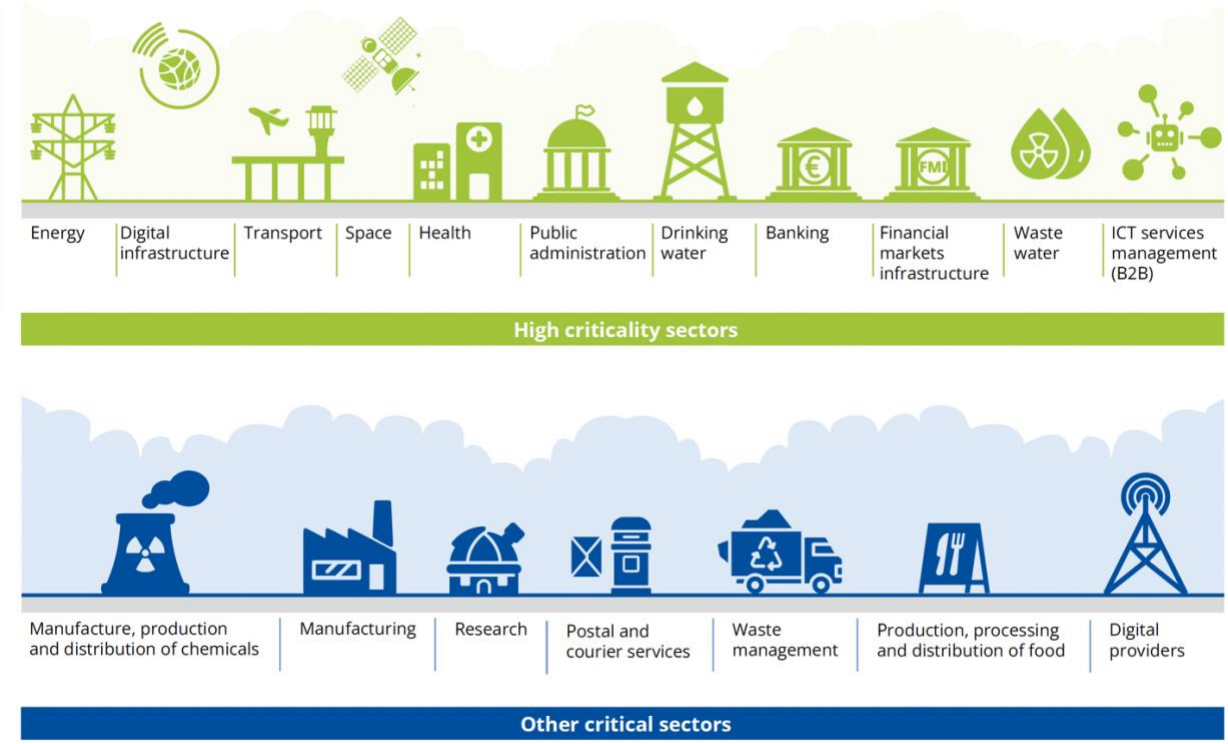


Gráfico elaborado por la ENISA, como parte de la campaña de información sobre la NIS2. Más información en www.enisa.europa.eu

Por qué el acceso remoto es el requisito más importante de NIS2

El punto de convergencia

La mayoría de las obligaciones de NIS2 pueden abordarse de forma relativamente aislada: los procesos de notificación de incidentes pueden definirse independientemente de las normas de cifrado, o las políticas de control de acceso pueden desarrollarse por separado de los procedimientos de gestión de vulnerabilidades. El acceso remoto es la excepción. Es el único ámbito en el que convergen simultáneamente los siguientes requisitos de NIS2:

- **Seguridad de la cadena de suministro** (artículo 21, apartado 2, letra d): porque el acceso remoto es la vía por la que proveedores, contratistas y terceros acceden a sus sistemas
- **Seguridad de la red y gestión de vulnerabilidades** (artículo 21, apartado 2, letra e): porque los protocolos de acceso remoto se encuentran entre los vectores de ataque más explotados
- **Cifrado** (artículo 21, apartado 2, letra h): porque cada sesión remota transmite datos sensibles a través de redes que pueden no estar bajo su control
- **Control de acceso y gestión de activos** (artículo 21, apartado 2, letra i): porque el acceso remoto es el punto de entrada donde deben aplicarse la identidad, la autenticación y los privilegios
- **Notificación de incidentes** (artículo 23): porque las sesiones de acceso remoto generan las pruebas de auditoría que respaldan las obligaciones de notificación en un plazo de 24 y 72 horas
- **Certificación de ciberseguridad** (artículo 24): porque las herramientas que gestionan el acceso remoto deben estar ellas mismas certificadas y ser auditables
- **Capacidades del CSIRT** (artículo 11): porque la visibilidad en tiempo real de las sesiones remotas es esencial para la detección de amenazas y la respuesta a incidentes

Ninguna otra capacidad por sí sola abarca tantos artículos de la normativa NIS2. Por eso el acceso remoto no es solo un elemento más de la lista de verificación de cumplimiento de la NIS2.

La realidad de la superficie de ataque

El acceso remoto es el principal vector de entrada para los ataques a la cadena de suministro contra infraestructuras críticas. Los mecanismos están bien documentados: credenciales de proveedores comprometidas, acceso VPN sin control, conexiones RDP no reguladas y cuentas anónimas o compartidas utilizadas por contratistas. Cada uno de ellos representa una vía directa hacia los sistemas que la NIS2 designa como esenciales.

El riesgo se ve agravado por lo que la NIS2 define como «cadena de suministro digital». Cualquier organización que cuente con un dispositivo con chip accesible de forma remota —desde ordenadores portátiles y servidores hasta robots de producción, sensores de la red eléctrica,

equipos médicos, sistemas de transporte autónomos e infraestructura satelital— tiene una superficie de ataque de acceso remoto que requiere gobernanza. Para las organizaciones de los sectores esenciales de la NIS2, esa superficie suele ser mucho mayor de lo que creen.

El alcance de los «equipos digitales» según la NIS2

Las obligaciones de la cadena de suministro de la NIS2 se aplican a cualquier dispositivo equipado con un microcontrolador o capacidad de procesamiento al que se pueda acceder de forma remota. Esto incluye no solo la infraestructura de TI , sino también la tecnología operativa (OT): sistemas de control industrial, dispositivos médicos, sistemas de gestión del transporte, sensores de la red eléctrica y equipos de defensa. Si tiene un chip y se puede acceder a él de forma remota, entra dentro del ámbito de aplicación.

El problema de las VPN

Muchas organizaciones siguen gestionando el acceso de terceros y proveedores a través de soluciones punto a red, como VPN o arquitecturas equivalentes a VPN, que conceden un amplio acceso a la red a los usuarios autenticados. Este enfoque es estructuralmente incompatible con los requisitos de seguridad de la cadena de suministro de NIS2.

Una VPN concede a un usuario conectado acceso a un segmento de red, no a un dispositivo o aplicación específicos. No puede hacer cumplir los principios de acceso «necesidad de conocer» o «necesidad de realizar» con el nivel de detalle que exige NIS2. No puede restringir el acceso por franjas horarias, certificar la autorización de la persona para una tarea específica ni generar las pruebas de sesión a prueba de manipulaciones necesarias para la notificación de incidentes. Según NIS2, el acceso a sistemas críticos basado en VPN es una vía de acceso no controlada.

El acceso remoto conforme a NIS2 requiere una arquitectura punto a punto: una conexión controlada, autenticada, supervisada y totalmente registrada entre una persona autorizada y un dispositivo específico, sin capacidad de movimiento lateral y sin presencia persistente en la red.

Vulnerabilidades en las cadenas de suministro digitales: acceso seguro de terceros

El acceso de terceros es su responsabilidad

En virtud de la NIS2, una organización es responsable del nivel de ciberseguridad de todos los proveedores o contratistas que tengan acceso a sus sistemas. La obligación de cumplimiento no se limita al perímetro de la organización, sino que se extiende a todos los terceros que puedan acceder a su interior. Considere la variedad de accesos remotos de terceros que son habituales en una organización sujeta a la NIS2: técnicos de soporte informático que acceden de forma remota a los dispositivos de los usuarios finales; proveedores de BPO que acceden a sistemas financieros y de ERP; ingenieros de OT que reconfiguran equipos industriales; fabricantes de dispositivos médicos que actualizan el firmware en sistemas hospitalarios; contratistas de defensa que acceden a la infraestructura de comunicaciones; consultores energéticos que leen datos de sensores de instalaciones de la red eléctrica. Cada una de estas interacciones debe estar controlada, autenticada, registrada y ser susceptible de revisión forense.

¿Quién tiene acceso a su cadena de suministro digital?

El primer paso para el cumplimiento de la normativa NIS2 en materia de acceso remoto es comprender quién tiene acceso remoto a qué sistemas. Para la mayoría de las grandes organizaciones, esto no es tan sencillo como parece. Las relaciones con los proveedores están documentadas en los sistemas de compras, pero los privilegios de acceso remoto a menudo se gestionan por separado, a veces por departamentos individuales o equipos de cada sede, sin una supervisión centralizada. El resultado es un panorama de accesos que se ha desarrollado de forma orgánica a lo largo de los años, con permisos que perduran más allá de los proyectos y las personas.

El artículo 22 de la NIS2 exige evaluaciones coordinadas de los riesgos de seguridad para las cadenas de suministro críticas. Esto requiere que las organizaciones identifiquen su cadena de suministro, identifiquen qué proveedores tienen acceso remoto y evalúen los riesgos asociados. Sin pruebas documentadas que respondan a la pregunta «¿quién tiene acceso remoto a qué sistemas?», no es posible cumplir con el artículo 22.

Requisitos de cumplimiento de la NIS2: Mapeo del acceso remoto

Temas de capacidades y cobertura de los artículos

La tabla siguiente relaciona las capacidades de acceso remoto de Netop con los artículos específicos de la NIS2 a los que se refieren. Esta estructura está diseñada para respaldar tanto las evaluaciones de cumplimiento como la documentación de auditoría, demostrando la conexión entre los controles operativos y las obligaciones reglamentarias.

Tema de capacidad	Artículo de la NIS2	Requisito abordado
Control de acceso y autenticación	Art. 21, apartado 2, letras d) e i)	Acceso con privilegios mínimos, MFA, identidad federada, eliminación del acceso anónimo
Supervisión y grabación de sesiones	Art. 21, apartado 2, letra e), art. 23	Registro de auditoría audiovisual a prueba de manipulaciones, registro de teclas y ratón, pruebas forenses para la notificación de incidentes
Gobernanza de la cadena de suministro digital	Art. 21, apartado 2, letra d), art. 22	Agrupación de accesos de proveedores, restricción de direcciones IP, restricciones de franjas horarias, supervisión de doble control, listas blancas geográficas
Cifrado e integridad de los datos	Art. 21, apartado 2, letra h)	Cifrado de extremo a extremo AES-256 para sesiones en tránsito y grabaciones en reposo; intercambio de claves Diffie-Hellman / RSA
Respuesta a amenazas en tiempo real	Art. 11, apartado 3, letra a)	Panel de control de terminales en tiempo real, interruptor de emergencia para sesiones no autorizadas, desactivación de permisos, compatibilidad con la visibilidad del CSIRT
Infraestructura certificada	Art. 24	ISO 27001, SOC 2, PCI-DSS, FIPS, HIPAA; residencia de datos en la UE en AWS; opciones de implementación local e híbrida
Soporte para la notificación de incidentes	Art. 23	Registro centralizado a nivel de entidad, integración con AWS CloudTrail, registros cifrados a prueba de manipulaciones para cumplir con las obligaciones de notificación de 24 h/72 h

Artículo 21: Medidas de gestión de riesgos en detalle

§2.d — Seguridad de la cadena de suministro

Las organizaciones deben controlar y restringir a qué pueden acceder los proveedores, cuándo pueden acceder y qué pueden hacer una vez conectados. Esto requiere una gestión de accesos con un nivel de granularidad que las herramientas genéricas de acceso a la red no pueden proporcionar.

- Los permisos de acceso deben definirse según principios de agrupación: nivel de criticidad, ubicación geográfica, certificaciones poseídas y necesidad de realizar la tarea
- Las restricciones de franja horaria deben ser exigibles: un contratista autorizado para una franja de mantenimiento específica no debería poder conectarse fuera de dicha franja
- Deben existir mecanismos de supervisión humana (el principio de los cuatro ojos) para las sesiones de alto riesgo, lo que requiere que un supervisor designado acepte o supervise la conexión
- El filtrado de IP debe restringir el acceso a rangos geográficos incluidos en la lista blanca y a direcciones de contratistas específicas
- Los permisos de acceso a nivel de aplicación deben ser aplicables, limitando lo que un usuario conectado puede ver e interactuar

§2.e — Seguridad de la red y gestión de vulnerabilidades

Los protocolos de acceso remoto se encuentran entre los vectores de ataque más frecuentemente explotados en infraestructuras críticas. El bloqueo de protocolos abiertos inseguros —RDP, VNC, Telnet y SSH— reduce sustancialmente la superficie de ataque. La sustitución del acceso punto a red por una arquitectura punto a punto elimina la capacidad de movimiento lateral que hace que las vulnerabilidades en la cadena de suministro sean tan perjudiciales.

- La grabación de sesiones debe capturar todos los eventos de teclado, vídeo y ratón, proporcionando pruebas de nivel forense de cada acción realizada durante una sesión remota
- Los protocolos de sesión remota abiertos deben bloquearse en el perímetro de la red
- El acceso punto a red basado en VPN o equivalente para proveedores externos debe sustituirse por un acceso controlado punto a punto
- Todo el registro debe realizarse a nivel de la entidad, y no solo a nivel de los dispositivos de los proveedores o contratistas; la organización debe ser la responsable del registro de auditoría

§2.h — Cifrado

Todos los datos transmitidos en una sesión remota, así como todas las grabaciones de sesiones almacenadas en reposo, deben cifrarse según un estándar reconocido. El cifrado AES de 256 bits para sesiones en tránsito, combinado con el intercambio de claves Diffie-Hellman o RSA, constituye el estándar reconocido, y acorde a la normativa, para las implementaciones de acceso remoto conformes.

§2.i — Control de acceso y seguridad de los recursos humanos

Debe eliminarse el acceso anónimo, incluidas las sesiones de solo lectura. Toda persona con acceso remoto, ya sea un empleado o un contratista externo, debe ser identificada y autenticada de forma fehaciente antes de que se establezca una sesión. La autenticación multifactorial es obligatoria para los sistemas conectados a Internet. La gestión federada de identidades garantiza que los derechos de acceso del personal que ha dejado la empresa o de los contratistas cuyos contratos han expirado se revoquen de inmediato.

- La integración de directorios de usuarios federados garantiza la gobernanza de identidades a gran escala
- La autenticación multifactorial (MFA) debe aplicarse antes de establecer cualquier sesión, no como una capa opcional
- El acceso a sesiones anónimas, compartidas o no solicitadas debe bloquearse para todas las categorías de usuarios

Artículo 23: Notificación de incidentes

La NIS2 exige que la notificación inicial a las autoridades nacionales se realice en un plazo de 24 horas tras un incidente significativo, y que se presente un informe completo en un plazo de 72 horas. Para las organizaciones que se enfrentan a un incidente relacionado con el acceso remoto, como pueden ser unas credenciales comprometidas de un contratista, una sesión no autorizada o un movimiento lateral, la capacidad de presentar pruebas documentadas dentro de estos plazos depende totalmente de la calidad de la infraestructura de auditoría implantada antes de que se produzca el incidente.

Las grabaciones de sesiones, los registros de conexión y los datos de eventos de acceso deben ser a prueba de manipulaciones, almacenarse en múltiples ubicaciones y ser accesibles a nivel de la entidad. Sin esta infraestructura implantada antes de un incidente, no se pueden cumplir los requisitos de notificación de 24 y 72 horas con el nivel de prueba exigido.

Artículo 11: Capacidades del CSIRT

Los equipos de respuesta a incidentes de seguridad informática (CSIRT) requieren visibilidad en tiempo real de la red y los sistemas de información que protegen. En el caso del acceso remoto, esto significa un panel de control en tiempo real que muestre todos los terminales en línea y fuera de línea, todas las sesiones activas, todas las conexiones en curso y todos los permisos actualmente implementados. La capacidad de «kill-switch» (la capacidad de terminar una sesión sospechosa al instante) no es una función de conveniencia; es un requisito operativo del artículo 11.

Cómo facilita Netop el cumplimiento

La infraestructura de cumplimiento que necesitan sus auditores

Cumplir los requisitos de acceso remoto de NIS2 no es principalmente un reto de políticas, sino un reto de infraestructura. Las políticas sin mecanismos de aplicación son insuficientes. Lo que los auditores de NIS2 exigen son pruebas: pruebas documentadas de que los controles están implementados, se aplican de forma coherente y generan registros aptos para auditorías. Netop es la infraestructura que genera esas pruebas.

Control de acceso y autenticación

Netop aplica un acceso granular y basado en roles a nivel de auditorías NIS2 individuales. Los permisos se definen por usuario, por grupo de dispositivos, por aplicación y por intervalo de tiempo. Cada sesión requiere una identificación positiva. No se permite el acceso anónimo para ninguna categoría de usuario. La autenticación multifactorial se aplica de forma nativa o mediante la integración con soluciones de identidad empresarial existentes. La compatibilidad con directorios federados garantiza que los derechos de acceso reflejen el estado actual de las relaciones entre contratistas y empleados, en lugar de instantáneas históricas.

Supervisión de doble control y supervisión humana

Para las sesiones remotas de alto riesgo, en particular aquellas realizadas por proveedores externos en equipos críticos, Netop admite mecanismos de control de calidad humanos. La aceptación de la sesión puede delegarse en un supervisor de seguridad designado: la sesión no continúa hasta que una persona autorizada la apruebe, ya sea a través de una ventana emergente en pantalla o de una confirmación por correo electrónico. Este principio de «cuatro ojos» aborda directamente los requisitos de seguridad de la cadena de suministro de NIS2 y proporciona un registro documentado de la aprobación de cada sesión supervisada.

Grabación de sesiones a prueba de manipulaciones

Todas las sesiones remotas en la plataforma Netop pueden grabarse con total fidelidad de audio y vídeo, incluyendo todos los eventos del teclado, los movimientos del ratón y la actividad de la pantalla, capturados en secuencia. Las grabaciones se almacenan en un formato cifrado y a prueba de manipulaciones con controles de acceso de solo lectura, lo que garantiza la preservación de la cadena de pruebas. En caso de incidente, estas grabaciones proporcionan la documentación de calidad forense necesaria para la presentación de informes según el artículo 23 y para las interacciones con los CSIRT nacionales y las autoridades de supervisión.

Las grabaciones utilizan códecs no estándar o cifrados para evitar la manipulación externa. Las sesiones se interrumpen automáticamente en caso de fallo en la grabación, lo que garantiza que ninguna sesión continúe sin que la capacidad de auditoría esté activa.

Gobernanza del acceso a la cadena de suministro

La arquitectura de Netop está diseñada específicamente para resolver el problema de acceso en la cadena de suministro al que se dirige la NIS2. Los proveedores externos, contratistas y prestadores de servicios solo acceden a los dispositivos y aplicaciones específicos para los que están autorizados, durante los intervalos de tiempo para los que han sido aprobados, y desde los rangos de IP en los que están registrados para su uso . El acceso no puede ampliarse más allá de estos parámetros sin una nueva autorización explícita.

- El «IP-fencing» restringe las sesiones a rangos geográficos incluidos en la lista blanca y a direcciones de proveedores específicas
- Los controles de intervalos de tiempo garantizan que el acceso de los contratistas caduque automáticamente al finalizar los periodos de contratación
- El acceso «necesario para el desempeño» limita lo que se puede ver y hacer durante una sesión, a nivel de aplicación
- Los mecanismos de aceptación de sesiones requieren aprobación humana para las conexiones sensibles

Visibilidad en tiempo real y kill switch

Netop ofrece un panel de control en tiempo real que proporciona al personal de operaciones de seguridad y del CSIRT una visibilidad completa del entorno de acceso remoto: qué terminales están en línea o fuera de línea, qué sesiones están activas, qué conexiones se están ejecutando y qué permisos están actualmente implementados. Las sesiones sospechosas pueden terminarse al instante. Los permisos pueden desactivarse en tiempo real sin necesidad de intervenir en el terminal.

Estándares de cifrado

Todas las sesiones remotas de Netop se cifran de extremo a extremo mediante AES-256. Se protegen tanto los datos de las sesiones en tránsito como las grabaciones almacenadas en reposo. El intercambio de claves utiliza algoritmos de exponenciación modular Diffie-Hellman o RSA, cumpliendo con los estándares reconocidos a los que se hace referencia en el artículo 21, apartado 2.h, de la NIS2.

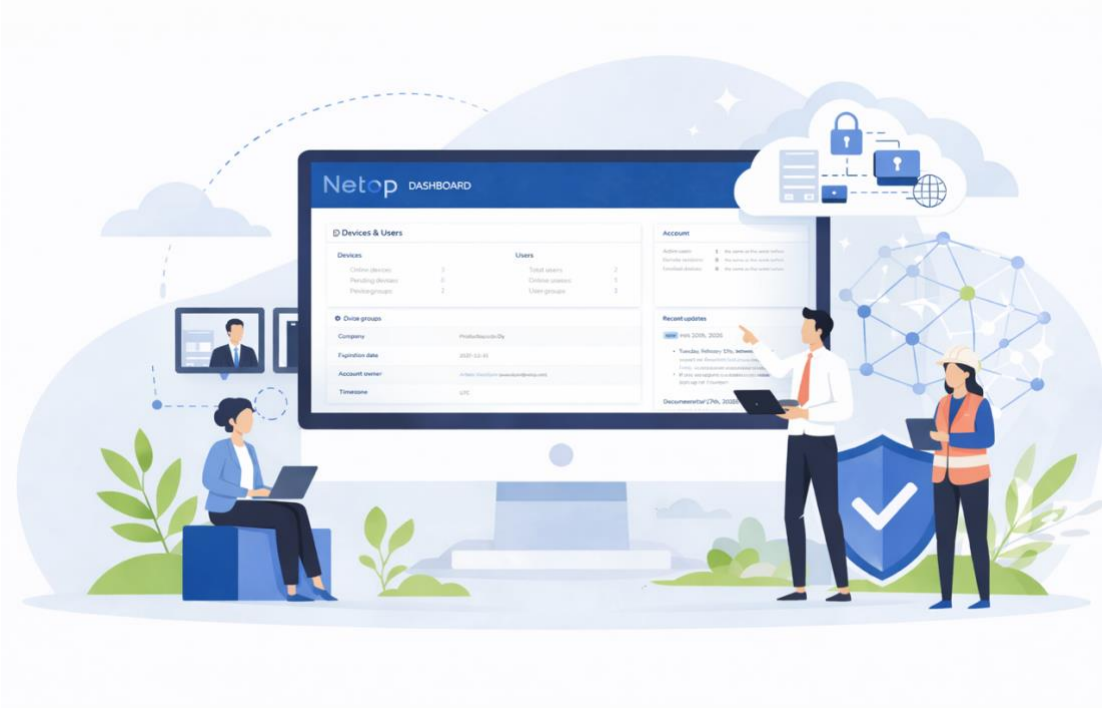
Control a nivel de hardware: integración con Intel AMT

Para las organizaciones con infraestructura habilitada para Intel vPro, la integración de Netop con Intel AMT amplía el acceso remoto seguro hasta el nivel del hardware. Esto incluye One-Click Recovery: un proceso remoto seguro, controlado por permisos y totalmente auditado para restaurar un dispositivo crítico para el negocio sin intervención física. Para los operadores de infraestructuras críticas que gestionan activos distribuidos geográficamente —como nodos de la red eléctrica, sistemas de gestión del transporte o equipos de comunicaciones de defensa—, esta capacidad reduce el riesgo operativo asociado a los escenarios de recuperación remota, al tiempo que mantiene el registro de auditoría exigido por la NIS2.

Bloqueo de vectores de ataque de protocolos abiertos

Netop recomienda y respalda el bloqueo de protocolos de sesión remota abiertos, como RDP, VNC, Telnet y SSH, en el perímetro de la red. Estos protocolos representan una superficie de ataque significativa y bien documentada. Su sustitución por una arquitectura de acceso remoto punto a punto, controlada y autenticada, reduce sustancialmente la superficie de amenaza y elimina la capacidad de movimiento lateral que caracteriza a los ataques a la cadena de suministro en infraestructuras críticas.

Acerca de Netop



Acceso remoto seguro para entornos críticos

Netop es un proveedor global de software de acceso remoto seguro para infraestructuras críticas, con más de 40 años de experiencia al servicio de sectores críticos para las empresas. Netop es utilizado por cientos de organizaciones en todo el mundo, lo que permite a técnicos, empleados, ingenieros, contratistas y subcontratistas acceder de forma controlada y remota a dispositivos críticos para las operaciones diarias y la resolución de problemas.

Sectores a los que presta servicio

Netop opera en todos los sectores esenciales e importantes de la NIS2, con especial profundidad en aquellos en los que el riesgo de acceso remoto es mayor:

- Defensa: acceso remoto seguro para contratistas de defensa, infraestructura de comunicaciones y equipos de misión crítica
- Energía: operaciones remotas para infraestructuras de red, sistemas de tuberías e instalaciones de energía renovable
- Gobierno y administración pública: acceso seguro para entidades de la administración pública central y regional
- Sanidad: acceso remoto a equipos médicos, sistemas de laboratorio e infraestructura clínica
- Transporte: gestión remota de sistemas de control del transporte, equipos de flotas e infraestructura logística
- Servicios financieros: acceso seguro a sistemas de negociación, redes de cajeros automáticos y operaciones financieras

- Fabricación y servicios públicos: acceso remoto a sistemas de control industrial, líneas de producción y tecnología operativa

Netop respalda y permite el cumplimiento de los principales marcos de seguridad, como ISO 27001, SOC 2, PCI-DSS, FIPS e HIPAA, a través de su arquitectura de seguridad, sus controles y su flexibilidad de implementación.

Producto diseñado para sistemas críticos que deben cumplir con la normativa

El mercado de las herramientas de acceso remoto es amplio, pero el cumplimiento de la NIS2 establece un listón alto y específico. La mayoría de los productos de acceso remoto se diseñaron pensando en la comodidad operativa: facilidad de conexión, compatibilidad multiplataforma y baja latencia. Netop se diseñó para entornos controlados en los que la seguridad, la auditabilidad y la gobernanza son imprescindibles. Esa diferencia de diseño es lo que importa en el marco de la NIS2.

1. Cobertura de controles NIS2 por diseño, no por adaptación

Netop se ajusta directamente a las medidas técnicas exigidas por NIS2: cifrado, control de acceso basado en roles, MFA, grabación de sesiones, integración SIEM y gobernanza del acceso a la cadena de suministro, ya que estas características se integraron en la arquitectura de la plataforma desde el principio. No son meros complementos de cumplimiento creados en respuesta a la normativa.

Netop puede demostrar la cobertura de los controles alineando capacidades específicas de la plataforma con artículos concretos de la NIS2. Esta distinción es importante en una auditoría: los auditores evalúan lo que un sistema hace realmente, no lo que un proveedor afirma que admite.

2. Arquitectura Zero Trust por diseño

La arquitectura de Netop incorpora de forma natural los principios de Zero Trust en tres áreas clave exigidas por la NIS2: verificar explícitamente (autenticación multifactorial, inicio de sesión único, autenticación con tarjeta inteligente), aplicar el principio del privilegio mínimo (control de acceso granular basado en roles, permisos basados en sesiones) y asumir la violación de seguridad (registro continuo, segmentación de la red, supervisión en tiempo real). Este enfoque difiere fundamentalmente de los productos que se limitan a superponer Zero Trust como una configuración sobre una arquitectura que no fue diseñada originalmente para ello.

3. Profundidad de la auditoría forense

El artículo 23 de la NIS2 exige que las organizaciones notifiquen los incidentes significativos, acompañados de pruebas documentadas, en un plazo de entre 24 y 72 horas. El estándar probatorio es estricto: no basta con demostrar que se produjo el acceso; las organizaciones deben poder demostrar con precisión ocurrió, cuándo y quién lo hizo. Netop ofrece capacidades completas de reproducción forense: grabaciones de sesiones a prueba de manipulaciones que incluyen todos los eventos del teclado, los movimientos del ratón y la actividad de la pantalla

capturados en secuencia, con retención configurable y almacenamiento cifrado de registros en múltiples destinos, como el almacenamiento local, SIEM y la nube.

> **La prueba forense**
> *¿Puede su herramienta de acceso remoto actual demostrar exactamente qué hizo un proveedor en un sistema en un momento específico de una fecha concreta? Si la respuesta es «tenemos registros, pero no reproducción de sesiones», eso es insuficiente para los requisitos de notificación del artículo 23 de NIS2 y de investigación forense.*

4. Control de acceso a la cadena de suministro

La seguridad de la cadena de suministro según el artículo 21, apartado 2, letra d), de la NIS2 exige que el acceso de terceros y proveedores se regule con un nivel de especificidad que las herramientas de acceso remoto de uso general no pueden proporcionar. Los controles de acceso a la cadena de suministro de Netop se encuentran entre sus principales elementos diferenciadores para los casos de uso de la NIS2:

- **Políticas de acceso específicas para cada proveedor**: definen quién puede acceder a qué, cuándo, desde dónde y durante cuánto tiempo
- **Acceso limitado en el tiempo y justo a tiempo**: acceso de contratistas que caduca automáticamente al final de un intervalo autorizado
- **Restricciones a nivel de aplicación**: limitan con qué puede interactuar un proveedor conectado durante una sesión, no solo a qué dispositivo puede acceder
- **Principio de los cuatro ojos**: exige que un supervisor designado acepte las sesiones de alto riesgo antes de que se lleven a cabo
- **Agrupación de dispositivos y usuarios por nivel de riesgo, ubicación geográfica y certificación**: permite la gestión del acceso a gran escala en amplias redes de proveedores

La mayoría de las herramientas de acceso remoto utilizan políticas de acceso uniformes para todos los usuarios. Ofrecen poca separación entre el acceso de los empleados internos y el de los contratistas externos, y proporcionan controles mínimos sobre lo que un proveedor conectado puede hacer durante una sesión. Según las normas de seguridad de la cadena de suministro de NIS2, esto constituye una brecha de cumplimiento estructural.

5. Flexibilidad de implementación y soberanía de los datos

Las organizaciones reguladas por NIS2 —especialmente en los sectores de defensa, administración pública e infraestructuras críticas— a menudo se enfrentan a requisitos de residencia de datos o mandatos de infraestructura que impiden opciones de implementación exclusivamente SaaS. Netop admite implementaciones locales, en la nube e híbridas, incluidos portales autohospedados y configuraciones de VPC. Netop Cloud opera en infraestructura de AWS dentro de la Unión Europea, lo que garantiza la residencia de datos en la UE para todos los datos de sesión, registros y grabaciones.

Las arquitecturas exclusivamente en la nube o con prioridad en la nube no son adecuadas para organizaciones con requisitos de soberanía. El principio fundamental es claro: la NIS2 hace

hincapié en el control. Las organizaciones no pueden reclamar el control total sobre su infraestructura de acceso remoto si dicha infraestructura está alojada en una nube de terceros que no gestionan.

6. Arquitectura de conexión inversa (solo saliente): sin superficie de ataque expuesta

Netop utiliza una arquitectura de conexión inversa: sin puertos de entrada abiertos, sin dependencia de RDP o VNC expuestos, sin infraestructura compartida que cree vías de ataque lateral. Todas las sesiones utilizan TLS con cifrado AES-256. Esta arquitectura aborda directamente los requisitos de reducción de riesgos de NIS2 según el artículo 21, apartado 2, letra e), y elimina los vectores de ataque más comúnmente explotados en ataques a la cadena de suministro contra infraestructuras críticas.

Las VPN combinadas con RDP siguen siendo un vector principal para los ataques a infraestructuras críticas. Las herramientas de acceso remoto que dependen de puertos de entrada abiertos o de una infraestructura de retransmisión compartida introducen una superficie de ataque que la arquitectura de Netop no presenta.

7. Compatibilidad con entornos heredados y de tecnología operativa (OT)

NIS2 abarca una amplia gama de equipos digitales, no solo terminales de TI modernos, sino también tecnología operativa: sistemas de control industrial, cajeros automáticos, dispositivos médicos, sensores de la red eléctrica, sistemas de gestión del transporte e infraestructura integrada que puede tener décadas de antigüedad. Netop está diseñado para funcionar en estos entornos, admitiendo sistemas heredados, condiciones de bajo ancho de banda y alta latencia, y escenarios de redes aisladas o restringidas.

La mayoría de las herramientas de acceso remoto están diseñadas para terminales de TI modernos y no funcionan bien, o no funcionan en absoluto, en entornos de TO y heredados. Para las organizaciones dentro del ámbito de aplicación de NIS2 que incluyen sistemas industriales o integrados (que constituyen la mayoría de las entidades esenciales en los sectores de la energía, el transporte y la fabricación), esto supone una limitación significativa en cuanto a su idoneidad.

Nota sobre la certificación NIS2

Actualmente, ningún proveedor de acceso remoto cuenta con una «certificación NIS2» formal, ya que dicha certificación aún no existe dentro del marco de la UE. La base adecuada para la comparación es la cobertura de capacidades: qué plataforma implementa los controles técnicos que exige la NIS2, con la profundidad de auditoría que exigen dichos requisitos, en los modelos de implementación aceptados por las organizaciones reguladas. Según estos criterios, la arquitectura y el conjunto de funciones de Netop se ajustan más directamente a los requisitos de la NIS2 que otras alternativas disponibles en el mercado.

Hoja de ruta paso a paso para la implementación del acceso remoto conforme a NIS2

El siguiente marco de cuatro pasos ofrece un enfoque estructurado para el cumplimiento de la normativa NIS2 en materia de acceso remoto. Está diseñado para generar la documentación necesaria tanto para el proyecto de implementación de Netop como para futuras auditorías de NIS2.

Paso 1: Mapear su cadena de suministro digital n

Elabore una lista exhaustiva de todos los proveedores, contratistas y prestadores de servicios con los que mantenga cualquier tipo de relación de servicios digitales. Recurra a los registros contables, los sistemas de compras y de gestión de relaciones con proveedores, así como a los contratos activos de los últimos 12 a 36 meses. El objetivo es crear un registro completo de proveedores, que no se limite a los proveedores de TI, sino que incluya cualquier organización que preste servicios que impliquen el acceso digital a sus sistemas.

En esta fase, los proveedores que no prestan servicios digitales (como la gestión de instalaciones, el transporte físico o el suministro de material de oficina) pueden excluirse del ámbito del acceso remoto. Los elementos restantes de la lista constituyen la base de la evaluación de la cadena de suministro.

Paso 2: Realice un inventario de su equipo digital

Cualquier dispositivo con un chip, un microcontrolador o capacidad de procesamiento al que se pueda acceder de forma remota entra dentro del ámbito de aplicación. Esto va mucho más allá de los activos de TI convencionales. Las fuentes para este inventario incluyen:

- **Activos de TI y comunicaciones:** ordenadores portátiles, ordenadores de sobremesa, servidores, equipos de red, infraestructura de comunicaciones
- **Automatización de edificios e instalaciones:** sistemas de control de acceso, videovigilancia, plataformas de gestión de edificios
- **Tecnología operativa específica del sector:** robots industriales, sensores, equipos médicos, cajeros automáticos, terminales de punto de venta, líneas de producción, vehículos de transporte, equipos de servicios municipales, controles de instalaciones energéticas

Los dispositivos a los que solo se puede acceder físicamente —y nunca de forma remota— pueden excluirse en esta fase. El resultado es un registro completo de equipos, con el estado de acceso remoto confirmado para cada elemento.

Paso 3: Mapear el acceso de los proveedores a los equipos

Con el registro de proveedores y el inventario de equipos a mano, el equipo del proyecto mapea quién accede a qué, en qué condiciones y desde dónde. Esto tiene dos dimensiones:

- Centrado en el proveedor: para cada proveedor, ¿a qué dispositivos acceden de forma remota, para qué servicios, desde qué ubicaciones y con qué frecuencia?
- Centrado en los dispositivos: para cada equipo, ¿qué usuarios o proveedores acceden a él de forma remota, desde qué redes (corporativa, externa, doméstica, Internet) y bajo qué control de acceso está actualmente en vigor?

El resultado de este paso es el mapa de acceso remoto seguro: una matriz documentada de usuarios, dispositivos, condiciones de acceso y estado actual del control. Este documento se convierte en la definición del alcance del proyecto de cumplimiento de la NIS2 y en la referencia de referencia para futuras auditorías.

Paso 4: Implementación con Netop

La documentación elaborada en los pasos 1 a 3 proporciona toda la información necesaria para la implementación de Netop. Cada vía de acceso de proveedores identificada en el mapa se configura en Netop con los controles de acceso, las ventanas de tiempo, las restricciones de IP, los ajustes de grabación y los requisitos de supervisión adecuados. La implementación sustituye las vías de acceso no controladas por conexiones reguladas, auditables y conformes con NIS2.

Tras la implementación, la plataforma Netop genera las pruebas de auditoría continuas (grabaciones de sesiones, registros de conexión, registros de eventos de acceso) que el cumplimiento de la NIS2 exige que se mantengan y puedan presentarse previa solicitud.

Costes del incumplimiento

Sanciones económicas

El artículo 34 de la NIS2 establece sanciones administrativas por infringir los artículos 21 y 23, es decir, las obligaciones de gestión de riesgos y presentación de informes que respaldan directamente la gobernanza del acceso remoto. La estructura de multas aplica el importe más alto entre un máximo fijo y un límite basado en el volumen de negocio.

Tipo de entidad	Multa máxima	Límite basado en el volumen de negocio	Artículos que dan lugar a multas
Entidades esenciales	10.000 .000 €	2 % de la facturación anual global	Art. 21 y 23
Entidades importantes	7.000.000 €	1,4 % de la facturación anual global	Art. 21 y 23

Para las grandes entidades esenciales de los sectores de la energía, las cadenas de suministro de defensa, la infraestructura financiera o la administración pública, una multa del 2 % de la facturación global no es un riesgo teórico, sino una exposición financiera significativa. Para una empresa con unos ingresos globales de 5.000 millones de euros, la exposición máxima solo en virtud de los artículos 21 y 23 es de 100 millones de euros.

Responsabilidad de la dirección

Más allá de las multas impuestas a la organización, la NIS2 introduce consecuencias personales directas para la alta dirección. En virtud del artículo 20, los órganos de dirección están obligados a supervisar la gestión de los riesgos de ciberseguridad y pueden ser considerados personalmente responsables de los fallos. En casos graves, esto puede incluir la suspensión de las funciones ejecutivas. La dimensión de la responsabilidad personal cambia el cálculo de la gobernanza: las decisiones en materia de ciberseguridad, incluida la gobernanza del acceso remoto, son ahora decisiones tomadas por el consejo de administración con responsabilidad individual asociada.

Consecuencias operativas y reputacionales

Las consecuencias de un fallo de seguridad en el acceso remoto en un sector esencial según la NIS2 van mucho más allá de las multas reglamentarias. Un operador de la red eléctrica cuya infraestructura de acceso remoto se vea comprometida se enfrenta a una interrupción operativa de los servicios esenciales. Un proveedor de asistencia sanitaria cuyo equipo médico sea accedido por un tercero no autorizado se enfrenta a un riesgo para la seguridad de los pacientes. Un contratista de defensa cuyo acceso remoto a sistemas sensibles sea vulnerado se enfrenta a implicaciones para la seguridad nacional.

El coste de la inacción

Para las organizaciones que aún no han abordado la gobernanza del acceso remoto en el marco de la NIS2: cada mes sin controles conformes es un mes de incumplimiento documentado al que pueden hacer referencia las autoridades supervisoras nacionales. La NIS2 no requiere que se produzca una violación para activar la aplicación de la normativa. Las revisiones y auditorías de las autoridades supervisoras pueden identificar controles inadecuados antes de que se produzca un incidente.

Conclusión

El acceso remoto no es un elemento más entre muchos en el marco de cumplimiento de la NIS2. Es el requisito que abarca la mayoría de las obligaciones, presenta el mayor riesgo operativo y suele ser el más deficiente en las organizaciones que han dependido de arquitecturas heredadas basadas en VPN o de acceso no controlado.

Para los operadores de infraestructuras críticas, las organizaciones de defensa y los organismos gubernamentales, el camino hacia el cumplimiento de la NIS2 en materia de acceso remoto implica cuatro pasos clave: saber quién tiene acceso a qué, aplicar controles detallados sobre ese acceso, crear evidencias a prueba de manipulaciones de cada sesión y ser capaz de responder a los incidentes y notificarlos con pruebas documentadas. Netop es el software diseñado para ofrecer estas cuatro funciones.

Las organizaciones que den el primer paso para implementar una gobernanza del acceso remoto conforme a la normativa no solo satisfarán a los auditores de NIS2, sino que también eliminarán una clase de riesgo de la cadena de suministro que representa uno de los vectores de ataque más explotados contra las infraestructuras críticas en la Europa actual.

Consulte con Netop sobre el cumplimiento de la NIS2

Solicite una demostración del software de acceso remoto seguro de Netop y comente sus requisitos de cumplimiento de la NIS2 con un especialista.

www.netop.com | info@netop.com

Apéndice: Sectores esenciales e importantes de la NIS2

Los siguientes sectores se definen en la Directiva (UE) 2022/2555 como entidades esenciales o importantes sujetas a las obligaciones de NIS2. Fuente: Comisión Europea / ENISA.

Sectores esenciales (de alta criticidad)

1. Energía: empresas eléctricas, operadores de distribución y transporte, oleoductos y gasoductos, producción y almacenamiento de hidrógeno
2. Transporte: compañías aéreas, infraestructura ferroviaria, transporte marítimo, gestión del tráfico rodado, sistemas de transporte inteligentes
3. Bancos y entidades de crédito
4. Infraestructuras de los mercados financieros: centros de negociación, contrapartes centrales
5. Sanidad: proveedores de asistencia sanitaria, laboratorios de referencia de la UE, fabricantes de productos farmacéuticos, fabricantes de productos sanitarios
6. Agua potable: proveedores y distribuidores de agua para consumo humano
7. Aguas residuales: empresas que recogen, eliminan o tratan aguas residuales
8. Infraestructura digital: puntos de intercambio de Internet, proveedores de DNS, registros de TLD, computación en la nube, centros de datos, redes de distribución de contenidos, proveedores de servicios de confianza, comunicaciones electrónicas públicas
9. Gestión de servicios de TIC (B2B): proveedores de servicios gestionados, proveedores de servicios de seguridad gestionados
10. Administración pública: entidades de la administración central y regional, tal y como las definan los Estados miembros
11. Espacio: operadores de infraestructuras terrestres que prestan apoyo a servicios espaciales

Otros sectores críticos (importantes)

12. Servicios postales y de mensajería
13. Gestión de residuos
14. Fabricación, producción y distribución de productos químicos
15. Producción, procesamiento y distribución de alimentos
16. Fabricación: dispositivos médicos, productos informáticos y electrónicos, equipos eléctricos, maquinaria, vehículos de motor y equipos de transporte
17. Proveedores digitales: mercados en línea, motores de búsqueda en línea, plataformas de redes sociales
18. Organizaciones de investigación

Fuente: Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo (Directiva NIS2). Texto oficial disponible en: eur-lex.europa.eu/eli/dir/2022/2555

Página de la Comisión Europea sobre la política NIS2: digital-strategy.ec.europa.eu/en/policies/nis2-directive