



Entendiendo la Directiva NIS 2



CONTENIDO DEL MANUAL

1. ¿Qué es la Directiva NIS 2?	5
2. ¿Qué ha cambiado?	9
3. ¿Cómo le va a afectar la Directiva NIS 2?	13
4. ¿Qué características del producto pueden ayudarle a mitigar las amenazas y protegerle contra los ataques?	17
5. Conclusión	19





¿Qué es la Directiva NIS 2?

La Directiva NIS, también conocida como Directiva (UE) 2016/1148, es una directiva de la UE que establece requisitos de ciberseguridad para los operadores de servicios esenciales y los proveedores de servicios digitales de la Unión Europea. La Directiva NIS tiene por objeto garantizar un alto nivel de seguridad de las redes y de la información en toda la UE, además de asegurar que los operadores de servicios esenciales y los proveedores de servicios digitales adopten las medidas adecuadas para gestionar el riesgo al que se pueden enfrentar sus redes y sistemas de información.

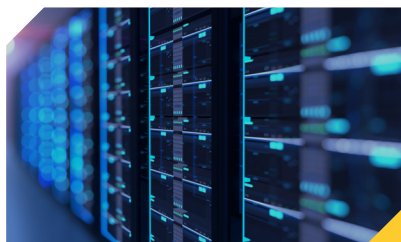
El 10 de noviembre de 2022, el Parlamento Europeo adoptó la Directiva NIS 2, que sustituye y deroga la Directiva NIS. La Directiva NIS 2 mejorará la gestión de los riesgos de ciberseguridad e introducirá obligaciones para informar en sectores como los de la energía, el transporte, la sanidad y las infraestructuras digitales. Los Estados miembros dispondrán de 21 meses a partir de la entrada en vigor de la Directiva para incorporar las disposiciones a sus legislaciones nacionales.

La Directiva NIS 2 tiene tres objetivos generales:



Ciberresiliencia

Aumentar la resistencia cibernética de una amplia gama de empresas con sede en la Unión Europea que operan en todos los sectores relevantes y realizan actividades esenciales.



Enfoque unificado

Reducir las contradicciones relacionadas con la resiliencia en el mercado interior en sectores actualmente cubiertos por la Directiva NSI, mediante la unificación de las capacidades en materia de ciberseguridad.



Establecimiento de procedimientos

Mejorar el conocimiento conjunto de la situación y de la capacidad colectiva de planificación y respuesta, impulsando el intercambio de información y estableciendo normas y procedimientos en caso de incidentes o crisis a gran escala.



Ambas directivas se centran en:

- > La adopción de medidas técnicas y organizativas para mejorar la seguridad de sus redes y sistemas informáticos.
- > La adopción de medidas adecuadas para prevenir incidentes de seguridad y/o minimizar su impacto para, de esta manera, garantizar la continuidad del servicio.
- > Comunicación a la autoridad competente, sin demoras indebidas, de cualquier incidencia en el servicio que tenga un impacto significativo en la continuidad del mismo.



2





¿Qué ha cambiado?

La nueva propuesta elimina la distinción entre Operadores de Servicios Esenciales (OES) y Proveedores de Servicios Digitales (DSP), determinando en su lugar las entidades como esenciales o importantes. También hay que señalar que, con la antigua Directiva NIS, los Estados miembros eran responsables de establecer qué entidades cumplían los criterios para ser consideradas operadores de servicios esenciales. La nueva Directiva NIS 2 introduce la regla del límite de tamaño como norma general para la identificación de las entidades reguladas. Esto significa que todas las entidades medianas y grandes que operen en los sectores o presten servicios cubiertos por la directiva se encontrarán dentro de su ámbito de aplicación.



Cambios adicionales



1. Se amplía el alcance de la Directiva NIS 2 para abarcar nuevos sectores (por ejemplo, los de gestión de aguas residuales, alimentación, espacio, etc.) en función de su importancia para la economía y la sociedad, incluyendo para esta finalidad a todas las medianas y grandes empresas de estos sectores. Al mismo tiempo, se garantiza a los Estados miembros flexibilidad a la hora de identificar entidades más pequeñas con un perfil de alto riesgo.

2. La creación, a través de la Agencia de Ciberseguridad de la Unión Europea (ENISA), de una Red Europea de Organización de Enlace para Ciber crisis (EU-CyCLONe) con el fin de apoyar la gestión coordinada de la ciberseguridad en incidentes y crisis a gran escala en la UE.

3. Se establece una mayor coordinación en la comunicación de nuevas vulnerabilidades descubiertas en toda la Unión Europea.

4. Se establece una lista de sanciones administrativas (similares a las del GDPR), incluyendo multas por incumplimiento de las obligaciones de notificación y gestión de riesgos para la ciberseguridad.

5. La propuesta incluye siete elementos que todas las empresas deben considerar o aplicar para reforzar sus requisitos de seguridad:

- Análisis de riesgos y políticas de seguridad de los sistemas de información
- Gestión de incidentes (prevención, detección y respuesta a incidentes)
- Continuidad de la actividad y gestión de crisis
- Seguridad de la cadena de suministro
- Seguridad en redes y sistemas de información
- Políticas y procedimientos para las medidas de gestión de los riesgos de ciberseguridad
- Uso de criptografía y cifrado

6. La propuesta introduce medidas de supervisión más estrictas para las autoridades nacionales, unos requisitos de aplicación más rigurosos y, además, pretende armonizar los regímenes sancionadores en los Estados miembros.

7. A escala europea, la propuesta refuerza la ciberseguridad de las tecnologías clave de la información y la comunicación. Los Estados miembros, en cooperación con la Comisión y la ENISA, tendrán que llevar a cabo evaluaciones de riesgos coordinadas de las cadenas de suministro críticas, basándose en el enfoque eficaz adoptado dentro del contexto de la Recomendación de la Comisión sobre Ciberseguridad de las Redes 5G.

8. La nueva Directiva se ha alineado con la legislación sectorial específica, en particular con la Ley de Resiliencia Operativa Digital (DORA), aplicable al sector financiero, y con la Directiva de Resiliencia de Entidades Críticas (CER), que refuerza la resiliencia de las entidades críticas que prestan servicios vitales de los que depende la subsistencia de los ciudadanos de la UE, como la energía, el transporte, la sanidad y el agua potable. De esta forma se garantizará la claridad jurídica y se asegurará la coherencia entre la NIS 2 y estas actuaciones.





¿Cómo le afectará la Directiva NIS 2?

La Directiva NIS exige que los OES y los DSP protejan sus recursos críticos para minimizar los riesgos que un incidente de seguridad supondría para la prestación de sus servicios. En teoría, cada organización sabe lo que es importante para prestar sus servicios y gestionar su negocio. Se podría argumentar que las tecnologías, como puede ser una cámara de vigilancia en red, no se clasifican como recursos críticos. Sin embargo, es importante tener en cuenta un enfoque holístico durante la determinación del ámbito. Algunos sistemas pueden presentar un riesgo, aunque estén fuera del ámbito establecido. Por ejemplo, aunque una cámara no sea esencial para el servicio, puede ser una fuente de vulnerabilidades que podría ser utilizada por un atacante para lanzar un ataque contra recursos críticos. Por lo tanto, es fundamental que los OES y los DSP valoren dichos riesgos durante su evaluación de la Directiva SRI.



Apoyo al cumplimiento

Con una mayor atención a la seguridad de la cadena de suministro, se espera que las organizaciones que necesiten cumplir la Directiva NIS 2 tengan que llevar a cabo un mayor grado de valoración con sus socios tecnológicos. Dentro de este proceso de evaluación y de una valoración del riesgo del proveedor, se espera que las políticas y los procesos desempeñen un papel más importante.

Demostración de la madurez cibernética

Proteger una red, sus dispositivos y los servicios que soporta requiere la participación activa de toda la cadena de suministro de los proveedores, así como de la organización del usuario final. Axis proporciona herramientas, documentación y formación para ayudar a mitigar los riesgos y mantener los productos y servicios de Axis siempre actualizados y protegidos. Axis dispone de una amplia lista de políticas y procesos, así como certificaciones de terceros.

Son las siguientes:

- Certificación ISO/IEC 27001 para nuestro Sistema de Gestión de la Seguridad de la Información (SGSI)
- Cyber Essentials Plus
- Modelo de Madurez para el Desarrollo de Software Seguro (BSIMM)
- El modelo de desarrollo de seguridad de Axis (ASDM): un marco que define el proceso y las herramientas utilizadas por Axis para crear software con seguridad integrada durante todo el ciclo de vida, desde el inicio hasta la desactivación.
- Axis es una Autoridad de Numeración CVE (CNA) bajo el dominio MITRE
- Política de gestión de vulnerabilidades
- Notificaciones de avisos de seguridad



Integridad de los productos de la cadena de suministro

La integridad del producto se consigue cuando el hardware y el firmware están protegidos satisfactoriamente contra cambios o manipulaciones no autorizados durante el recorrido del producto a través de la cadena de suministro. Junto con nuestros proveedores y partners en fabricación, Axis realiza multitud de controles de calidad para mantener y proteger la integridad de sus productos. Por ejemplo:

- El sistema de gestión de la seguridad de la información (SGSI) de Axis cuenta con la certificación ISO 27001, lo que significa que sigue procesos y buenas prácticas reconocidos internacionalmente en la gestión de la sistemas e infraestructura de información que ofrecen soporte al recorrido del producto a través de la cadena de suministro.
- Aplica el concepto de Confianza Cero, que se basa en el principio de nunca confiar y siempre verificar, independientemente de si son las personas o las máquinas las que se conectan tanto a las redes y arquitecturas como si se encuentran dentro de ellas.
- Los componentes siempre proceden de un proveedor incluido en la lista de proveedores autorizados, siguiendo el listado de materiales especificados por Axis.
- El proveedor no podrá modificar las especificaciones críticas de producción sin la autorización de Axis. Cualquier cambio aprobado debe documentarse y registrarse.
- Un proceso para la manipulación de materiales garantiza siempre el estado de los materiales, indicando cualquier variación que pudiera poner en peligro la calidad.
- Axis desarrolla, produce y suministra el equipo de producción crítico y el sistema de pruebas subyacente, además del sistema para probar los componentes, módulos y productos en los distintos niveles durante la producción. Esto limita los riesgos asociados a la manipulación. Axis proporciona una lista de funciones de seguridad mejoradas integradas.
- ARTPEC® son los chipsets del sistema en chip (SoC) desarrollados internamente por Axis que cumplen con la Ley de Autorización de Defensa Nacional (NDAA) de EE.UU. ARTPEC incorpora funciones de seguridad exclusivas para los dispositivos Axis, incluyendo el firmware firmado – que garantiza que sólo se pueda instalar firmware seguro autorizado– y el arranque seguro – que impide el arranque de firmware no autorizado..
- Para mejorar aún más los controles de seguridad, todos los datos de las pruebas se comparten con Axis de forma permanente 24/7 desde nuestros partners de producción, por lo que las modificaciones no autorizadas pueden identificarse inmediatamente.
- Se exige a los proveedores y partners fabricantes mantener un sistema que garantice la trazabilidad de los lotes producidos, desde el material entrante hasta la pieza acabada. Durante la producción, la pieza determinada se someterá a múltiples pruebas, como el Control de Calidad de Entrada (IQC) y la Inspección Óptica Automática (AOI), para comprobar que no se montan componentes falsificados.



4



¿Qué características del producto pueden ayudar a mitigar las amenazas y garantizar la protección contra los ataques?

Esta sección describe algunas de las funciones de seguridad avanzadas disponibles en los productos Axis



Firmware firmado

El firmware firmado lo implementa el proveedor de software y consiste en firmar la imagen del firmware con una clave privada. Cuando el firmware tiene esta firma adjunta a él, un dispositivo validará el firmware antes de aceptar la instalación. Si el dispositivo detecta que la integridad del firmware está en peligro, la actualización del firmware será rechazada.

Arranque seguro

El arranque seguro es un proceso de arranque que consiste en una cadena ininterrumpida de software validado criptográficamente, que comienza en una memoria inmutable (ROM de arranque). El arranque seguro se basa en el uso de firmware firmado y garantiza que un dispositivo sólo pueda arrancar con firmware autorizado.

Axis Edge Vault

Axis Edge Vault es un módulo informático criptográfico seguro que puede utilizarse para operaciones criptográficas en certificados almacenados de forma segura. Edge Vault proporciona almacenamiento protegido contra manipulaciones, lo que permite a cada dispositivo proteger sus secretos y establece una base para la implementación segura de funciones de seguridad más avanzadas.

ID del dispositivo Axis

El ID del dispositivo Axis funciona como un pasaporte digital y es único para cada unidad de dispositivo. Se almacena de forma segura y permanente en Edge Vault como un certificado, firmado por el certificado raíz de Axis. El ID del dispositivo Axis ha sido diseñado para demostrar el origen del dispositivo, lo que permite un nuevo nivel de confianza del dispositivo en el ciclo de vida del producto.

Almacenamiento seguro de claves con un módulo de plataforma de confianza (TPM)

Un módulo de plataforma de confianza (TPM) es un componente que proporciona un determinado conjunto de características criptográficas adecuadas para proteger la información frente accesos no autorizados. La clave privada se almacena en el TPM y nunca sale de él. Todas las operaciones criptográficas que requieren el uso de la clave privada se envían al TPM para ser procesadas. De esta manera se garantiza que la parte secreta del certificado nunca abandona el entorno seguro dentro del TPM y permanece a salvo incluso en caso de una brecha de seguridad.

Vídeo firmado

El vídeo firmado garantiza que se pueda verificar que las pruebas de vídeo no han sido manipuladas sin necesidad de demostrar la cadena de custodia del archivo de vídeo. Cada cámara utiliza su ID del dispositivo Axis único, guardado de forma segura en Axis Edge Vault, para incorporar una firma a la secuencia de vídeo. Cuando se reproduce el vídeo, el reproductor de archivos muestra si el vídeo está intacto. El vídeo firmado permite rastrear el vídeo hasta la cámara de origen y verificar que el vídeo no se ha modificado ni editado y que sigue estando en su forma original intacta y sin alterar.

HTTPS habilitado

HTTPS está habilitado por defecto con un certificado autofirmado desde AXIS OS 7.20. De esta forma se permite establecer la contraseña del dispositivo de forma segura. En AXIS OS 10.10 y posteriores, el certificado autofirmado se ha sustituido por el certificado de identificación de dispositivo seguro IEEE 802.1AR.



A continuación, se incluye un listado de las herramientas y guías de Axis para ofrecer apoyo al proceso de instalación, puesta en marcha y mantenimiento:

Guía de endurecimiento (Hardening Guide)

Para estructurar nuestras recomendaciones dentro del contexto de un marco de ciberseguridad, Axis ha optado por seguir los métodos descritos en la versión 8 de los Controles CIS, presentados por el Centro para Seguridad de Internet (CIS). Anteriormente conocidos como SANS Top 20 Critical Security Controls, los controles CIS proporcionan 18 categorías de Controles Críticos de Seguridad (CSC) creados para ocuparse de los tipos de riesgo de ciberseguridad más habituales que pueden afectar a una organización. Esta información puede encontrarse en la guía Axis Hardening.

Administrador de dispositivos AXIS (Axis Device Manager)

AXIS Device Manager es la herramienta de referencia para instalar y configurar nuevos dispositivos de forma rápida y sencilla. Ofrece a los instaladores de soluciones de seguridad y a los administradores de sistemas una herramienta muy eficaz para gestionar todas las principales tareas de instalación, seguridad y mantenimiento, tanto una a una como por lotes. Ésta es la forma más eficaz de realizar un seguimiento de los dispositivos Axis en una red, además de implementar políticas de seguridad en todos los dispositivos y llevar a cabo todas las actualizaciones de firmware de forma rápida y eficaz.

Conclusión

Aunque es muy poco probable que los sistemas de seguridad se clasifiquen como recursos críticos, es importante que los OES y los DSP consideren un enfoque holístico durante la determinación del alcance. Esto significa que las tecnologías de seguridad física deben evaluarse minuciosamente como parte de una valoración de la Directiva NIS 2 para poner de relieve cualquier riesgo potencial.

Axis adopta una visión completa de 360 grados en relación a su oferta de ciberseguridad. Los productos se diseñan con funciones integradas para hacer frente a los problemas de ciberseguridad, mientras que una amplia lista de políticas y procesos, herramientas, documentación y formación sirven de ayuda para mitigar los riesgos para mantener siempre protegidos a los clientes.

Acerca de Axis Communications

Axis hace posible un mundo más inteligente y seguro, creando soluciones para mejorar la seguridad y el rendimiento empresarial. Axis es una empresa de tecnología de redes líder del sector y ofrece soluciones de videovigilancia, control de acceso, porteros automáticos y sistemas de audio. Estas soluciones se ven mejoradas con aplicaciones analíticas inteligentes y cuentan con el soporte de una formación de alta calidad.

Axis cuenta con unos 4.000 empleados especializados en más de 50 países y colabora con partners tecnológicos y de integración de sistemas de todo el mundo para ofrecer soluciones a sus clientes. Axis se fundó en 1984 y su sede central se encuentra en Lund (Suecia).