DOCUMENTO TÉCNICO

NIS 2

Junio 2024

Índice

1 Introducción

1.1 ¿Qué es la directiva NIS 2?

NIS 2 es una directiva de la UE que debe transponerse a la legislación nacional de cada estado miembro de la UE antes del 17 de octubre de 2024. Su objetivo es alcanzar un alto nivel de ciberseguridad en toda la UE, con el fin de contribuir a la seguridad de la región y al buen funcionamiento de su economía y sociedad. Obliga a las entidades que prestan servicios esenciales e importantes en sectores clave de la sociedad a desarrollar mecanismos de ciberseguridad, mitigar las amenazas a los sistemas de redes y de información, garantizar la continuidad de los servicios en caso de incidentes y notificar incidentes de seguridad a las autoridades competentes. Exige a los estados miembros que adopten estrategias nacionales en materia de ciberseguridad y creen autoridades, como organismos de gestión de cibercrisis y equipos de respuesta ante incidentes de ciberseguridad. Esboza medidas para la gestión de los riesgos de ciberseguridad, así como medidas para su aplicación. Su incumplimiento por parte de entidades esenciales e importantes pueden acarrear cuantiosas multas y derivaciones de carácter jurídico para los equipos de gestión.

Para más información, visite:
eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 ¿A quién afecta la Directiva NIS 2?

La Directiva NIS 2 afecta a todas las entidades que prestan servicios **esenciales** o **importantes** a la economía y la sociedad europeas, incluidas empresas y proveedores.

1.2.1 Afectados directamente

Entidades esenciales – Energía, transporte, banca/finanzas, atención sanitaria, agua potable, aguas residuales, infraestructuras digitales, administración pública, sector aeroespacial

Entidades importantes – Servicios postales, gestión de residuos, industria química, alimentación, fabricación (por ejemplo, dispositivos médicos, equipos eléctricos y de transporte), proveedores digitales (por ejemplo, marketplaces online, motores de búsqueda, redes sociales), organizaciones de investigación.

Autoridades nacionales competentes – Los estados miembros de la UE designan a las autoridades nacionales competentes para supervisar la aplicación y el cumplimiento de la Directiva NIS 2 en sus respectivos países.

1.2.2 Afectados indirectamente

Proveedores – La Directiva NIS 2 afecta indirectamente a los proveedores y prestadores de servicios externos que proporcionan servicios esenciales o servicios digitales a entidades esenciales e importantes. Estas empresas deben garantizar la seguridad de sus productos y servicios, y pueden estar sujetas a requisitos contractuales sobre ciberseguridad por parte de sus clientes.

Usuarios de servicios esenciales y servicios digitales – Aunque no están directamente regulados por la Directiva NIS 2, los usuarios de servicios esenciales y servicios digitales se benefician de la mejora de las prácticas de ciberseguridad y de la capacidad de respuesta ante incidentes que exige la directiva. Esta circunstancia aumenta indirectamente la seguridad y fiabilidad de los servicios que utilizan.

2 Requisitos de la NIS 2

2.1 Para entidades esenciales e importantes

Medidas de seguridad – Aplique las medidas de seguridad adecuadas para gestionar los riesgos y garantizar la seguridad de sus redes y sistemas de información. Estas medidas deben basarse en evaluaciones de riesgos y en las prácticas recomendadas.

Informes de incidentes – Informe a las autoridades competentes de los incidentes significativos que puedan tener un impacto considerable en la seguridad de sus redes y sistemas de información. Informar a tiempo es esencial para coordinar las respuestas y mitigar los posibles perjuicios.

Gestión de riesgos – Realice evaluaciones de riesgos para identificar posibles amenazas y vulnerabilidades, y adopte medidas para mitigarlos.

Cooperación con las autoridades competentes – Coopere con las autoridades competentes designadas por los estados miembros de la UE. Esta medida incluye la obligación de proporcionar la información y el acceso necesarios a los sistemas con fines de supervisión y respuesta a incidentes.

Planificación de la respuesta ante incidentes – Desarrolle y actualice planes de respuesta ante incidentes para garantizar una actuación eficaz en caso de incidentes de ciberseguridad. En estos planes se deben esbozar los procedimientos de detección, notificación y mitigación de incidentes.

Seguridad de las cadenas de suministro – Proteja las cadenas de suministro, incluidos los proveedores externos, para garantizar la resiliencia general de la red y los sistemas de información.

Supervisión continua – Implemente mecanismos de supervisión y auditoría continuos de los sistemas de redes e información para detectar y responder a las amenazas y vulnerabilidades en tiempo real.

3 Impacto en los proveedores

Los proveedores pueden apoyar las entidades sujetas a la NIS 2 cumpliendo los siguientes requisitos:

Seguridad desde el diseño – Los fabricantes de dispositivos IoT deben incorporar funciones de seguridad en sus dispositivos desde la fase de diseño para que la seguridad sea una parte esencial del producto.

Actualizaciones y parches periódicos – Los fabricantes deben publicar periódicamente actualizaciones y parches de seguridad para solucionar las vulnerabilidades de sus dispositivos IoT.

Autenticación y autorización – Los dispositivos IoT deben utilizar mecanismos de autenticación eficaces y controles de autorización adecuados para impedir el acceso sin autorización.

Cifrado de datos – Hay que cifrar la información delicada que transmiten o almacenan los dispositivos IoT y evitar que sea interceptada por personas no autorizadas o que estas tengan acceso a la misma.

Informes de incidentes – Los fabricantes deben informar de cualquier incidente o brecha de seguridad relevantes en relación con sus dispositivos IoT a las autoridades pertinentes y, en su caso, a los consumidores o clientes.

Consideraciones sobre la privacidad – Los dispositivos IoT que procesan datos personales deben cumplir las normativas de protección de datos, como el RGPD (Reglamento General de Protección de Datos), además de la NIS 2.

Seguridad de la cadena de suministro – Hay garantizar la seguridad de toda la cadena de suministro, desde los proveedores de componentes hasta los clientes, para evitar la introducción de vulnerabilidades de seguridad en cualquier punto del proceso de producción.

4 La respuesta de Axis

A continuación se explica cómo Axis, en calidad de proveedor, cumple los requisitos establecidos por la NIS 2 para las entidades:

4.1 Seguridad desde el diseño

La seguridad desde el diseño es el modelo adoptado para garantizar que las consideraciones y actividades de seguridad se tienen en cuenta en el proceso de diseño y desarrollo del producto, con el objetivo de reducir el riesgo de vulnerabilidades y tener configuraciones con los máximos niveles de seguridad en los productos de forma predeterminada. En Axis, el principio de seguridad desde el diseño se aplica al software y al hardware, y se plasma a través de los elementos siguientes:

- *Modelo de desarrollo de seguridad de Axis (ASDM)*: ASDM es un marco con determinados procesos y herramientas definidos para tener en cuenta las consideraciones de seguridad en todo el proceso el desarrollo del software. Entre las actividades llevadas a cabo encontramos evaluaciones de riesgos, creación de modelos de amenazas, pruebas de penetración, análisis de vulnerabilidades y gestión de incidentes, así como un programa de recompensas por detección de fallos. Los desarrolladores de software de Axis utilizan ASDM para garantizar la integración de la seguridad en el desarrollo de software y reducir así el riesgo de publicar software con vulnerabilidades.
- *Programa de recompensas por detección de fallos*: Axis apoya un programa privado de recompensas por detección de fallos que refuerza las iniciativas de la empresa para identificar, subsanar y divulgar de forma proactiva las vulnerabilidades de AXIS OS, el sistema operativo basado en Linux que utilizan la mayoría de los productos de Axis. Refuerza el compromiso de Axis de forjar relaciones profesionales con investigadores de seguridad externos y hackers éticos.
- *Lista de materiales de software (SBOM)*: Axis genera una SBOM para AXIS OS, el sistema operativo basado en Linux utilizado en la mayoría de los dispositivos Axis. Pone en manos de los investigadores de seguridad, las autoridades y los clientes información sobre los componentes de software que integran AXIS OS. Resulta especialmente útil para los especialistas en evaluación de vulnerabilidades y análisis de amenazas, y es una muestra del compromiso de Axis con la transparencia en materia de ciberseguridad.
- *Ajustes de seguridad predeterminados de AXIS OS*: Los dispositivos que utilizan las últimas versiones de AXIS OS vienen preconfigurados de fábrica con las siguientes opciones: sin contraseña predeterminada; HTTP y HTTPS activados; incorporación y comunicaciones seguras con IEEE 802.1X/802.1AR/802.1AE activados por defecto; protocolos poco seguros desactivados. Encontrará más información sobre los controles de protección predeterminados *aquí*.
- *Axis Edge Vault*: Integrada en los dispositivos Axis, Axis Edge Vault es una plataforma de seguridad basada en el hardware que incluye funciones para proteger la integridad de los productos de red Axis y permitir la ejecución de operaciones seguras basadas en claves criptográficas. Protege la cadena de suministro de las siguientes formas: arranque seguro y sistema operativo firmado; identidad de dispositivo de confianza con el ID de dispositivo Axis único integrado para demostrar el origen del dispositivo; almacenamiento seguro de claves para impedir la manipulación de información criptográfica guardada y detección de la manipulación del vídeo con el vídeo firmado.

4.2 Actualizaciones y parches periódicos

Axis proporciona actualizaciones de software para abordar, entre otras cosas, las vulnerabilidades de seguridad descubiertas recientemente en sus productos de hardware y software. Axis también cuenta con herramientas de gestión de dispositivos para ayudar a los clientes a tener actualizado el software de los dispositivos Axis. Las nuevas versiones de AXIS OS para dispositivos conectados aparecen destacadas en AXIS Companion, AXIS Camera Station y aplicaciones de software de gestión de vídeo de socios como Milestone XProtect® y Genetec™ Security Center, así como en las herramientas de gestión de dispositivos Axis. Además, Axis ofrece un servicio de notificaciones de seguridad por suscripción abierto a todo el mundo. A continuación tiene información más detallada.

- *AXIS OS*: Axis ofrece dos alternativas principales para mantener actualizado el software del dispositivo: el modelo activo y el modelo de soporte a largo plazo (LTS). El modelo activo permite acceder a las últimas funciones, así como correcciones de errores y parches de seguridad. El software que funciona con modelos de soporte a largo plazo (LTS) permite disfrutar de la máxima la estabilidad: solo ofrece correcciones de errores y parches de seguridad, puesto que lo prioritario es tener un sistema de terceros bien integrado.
- Herramientas de gestión de dispositivos: *AXIS Device Manager* y *AXIS Device Manager Extend* son herramientas que ayudan a los clientes a tener actualizado el software de los dispositivos Axis con los últimos parches de seguridad y correcciones de errores.

  Para una configuración y gestión eficaces de los dispositivos Axis en local, AXIS Device Manager permite procesar por lotes de tareas de seguridad como la gestión de las credenciales de los dispositivos, la implementación de certificados, la desactivación de servicios no utilizados y la actualización de AXIS OS.

  AXIS Device Manager Extend incorpora un panel global con información sobre todos sus dispositivos e instalaciones en una única aplicación muy fácil de usar. El sistema le avisará cuando haya actualizaciones de software de los dispositivos disponibles y podrá realizar actualizaciones y otras tareas por lotes. También recibirá recomendaciones sobre productos de sustitución. Todas las actividades se pueden rastrear, y la información de los dispositivos del sistema se puede exportar para crear informes o con fines de auditoría.
- *Servicio de notificaciones de seguridad de Axis*: Este servicio envía a los suscriptores notificaciones sobre incidentes de seguridad y vulnerabilidades. Axis recomienda a todos los usuarios que se suscriban.

4.3 Autenticación y autorización

Para evitar accesos no autorizados y aumentar la seguridad general de sus dispositivos, Axis admite:

- Derechos de acceso a la gestión de dispositivos basados en roles (administrador/operador/visionador) y la posibilidad de centralizar la autenticación/autorización mediante la conexión de dispositivos Axis a integraciones de *Active Directory Federation Service* (ADFS) estandarizadas por TI. (ADFS es un componente de software desarrollado por Microsoft para ofrecer un servicio de autorización de inicio de sesión único (SSO) a usuarios de sistemas operativos Windows Server. ADFS permite a los usuarios en cualquier punto de la organización acceder a aplicaciones de sistemas operativos Windows Server utilizando unas únicas credenciales para el inicio de sesión).
- Tecnologías que facilitan las *redes de confianza cero* . En las últimas versiones de AXIS OS, estas tecnologías incluyen IEEE 802.1X, junto con ID de dispositivos Axis conformes con IEEE 802.1AR, para la incorporación automática y segura de dispositivos a una red IEEE 802.1X, e IEEE 802.1AE (MACsec) para el cifrado automático de la comunicación de datos.

4.4 Cifrado de datos

Para evitar que personas no autorizadas intercepten o accedan a información confidencial, los productos de Axis son compatibles con:

- HTTPS, donde todas las comunicaciones de datos son compatibles con TLS 1.2 o estándares más recientes. La conexión de transmisión de vídeo entre el servidor de software de gestión de vídeo AXIS Camera Station y el cliente está cifrada mediante AES-256.
- *IEEE 802.1AE (MACsec)* para el cifrado automático de la comunicación de datos.
- Transmisión segura de vídeo a través de RTP, también denominada SRTP/RTSPS (a partir de AXIS OS 7.40). SRTP/RTSPS utiliza un método de transporte cifrado seguro de extremo a extremo para garantizar que solo los clientes autorizados reciban la transmisión de vídeo del dispositivo Axis.
- *Cifrado del almacenamiento local* (tarjeta SD)
- *Exportación cifrada mediante contraseña de grabaciones locales* (tarjeta SD, información compartida a través de la red), a partir de AXIS OS 10.10. Esto significa que es posible exportar una grabación cifrada mediante contraseña, sumado a la posibilidad de compartir de forma segura datos de vídeo confidenciales sin necesidad de cifrar manualmente las grabaciones exportadas.

4.5 Informes de incidentes

Axis publica informes de incidentes de seguridad o vulnerabilidades descubiertas en nuestros productos y servicios.

- Axis es una autoridad de numeración de vulnerabilidades y exposiciones comunes (CVE). Esto significa que Axis sigue las prácticas recomendadas del sector en la gestión y respuesta —con transparencia— a las vulnerabilidades descubiertas en nuestros productos y servicios con el objetivo de minimizar el riesgo de exposición de los clientes. Axis también puede asignar números CVE a las vulnerabilidades que se acaban de descubrir y registrarlas en el sitio web *www.cve.org*. La *política de gestión de vulnerabilidades* de Axis está publicada en axis.com.
- Cualquiera puede suscribirse al servicio desde *aquí* para recibir notificaciones de seguridad de Axis.
- Las nuevas versiones de AXIS OS incluyen parches de seguridad y correcciones de errores. También se indica que hay software actualizado en AXIS Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend y en VMS de terceros como Milestone XProtect y Genetec Security Center.
- Axis está comprometida con la transparencia en relación con cualquier ciberataque a empresas e informará de dichos incidentes conforme a las directrices proporcionadas por las autoridades suecas pertinentes.

4.6 Consideraciones sobre la privacidad

Axis publica su *política de privacidad* y su aviso de privacidad en internet, donde explica qué datos personales se recopilan (por ejemplo, en una cuenta online en My Axis) y cómo se utilizan.

Axis también ha publicado su *marco y prácticas en materia de ciberseguridad* en relación con su Sistema de Gestión de Seguridad de la Información, que cuenta con la certificación ISO/IEC 27001. El ámbito de aplicación del certificado ISO/IEC 27001 de Axis abarca el desarrollo y las operaciones de la infraestructura y el servicio de TI internos. ISO 27001 es una norma reconocida internacionalmente que ofrece orientación

sobre cómo proteger y gestionar la información de una organización mediante una gestión eficaz de los riesgos.

La conformidad con la norma *ISO/IEC 27001* demuestra que Axis aplica procesos y prácticas reconocidos internacionalmente para gestionar su infraestructura y sus sistemas de información internos, utilizados para prestar sus servicios a clientes y socios.

Axis también ayuda a los clientes a abordar los problemas de privacidad en el ámbito de la vigilancia con respecto a la captura de vídeo y audio. Las soluciones incluyen:

- Uso de máscaras de privacidad estáticas en cámaras Axis y máscaras de privacidad dinámicas con la aplicación de software *AXIS Live Privacy Shield*.
- Analítica en el extremo, como la aplicación *AXIS People Counter* o *AXIS P8815-2 3D People Counter*, que solo capturan y almacenan datos numéricos estadísticos, sin que se procese ninguna información personal identificable.
- *Cámaras térmicas*
- *Productos de radar*
- Herramienta para aplicar máscaras en objetos o áreas sin interés de vídeos en *AXIS Camera Station*
- *Funciones de audio desactivadas por defecto* en los productos de videovigilancia Axis

Encontrará más información sobre las soluciones de privacidad en *axis.com/solutions/privacy-in-surveillance*

4.7 Seguridad de la cadena de suministro

Proteger la cadena de suministro, desde los proveedores de componentes hasta los clientes, es importante para evitar la introducción de vulnerabilidades de seguridad.

Axis apuesto por un *enfoque basado en el ciclo de vida* del producto a la hora de abordar la ciberseguridad. Nos comprometemos a mitigar los riesgos, no solo en toda la cadena de suministro, desde los componentes hasta el producto acabado, sino también durante la distribución y la implantación, así como en las fases de servicio y desinstalación.

A continuación se indican algunas estrategias aplicadas por Axis para garantizar la seguridad de la cadena de suministro:

- Axis compra los componentes críticos directamente a proveedores estratégicos. Colaboramos estrechamente con los socios que se dedican a la fabricación. Los procesos de producción se controlan y se comparten los datos con Axis las 24 horas del día, lo que permite un análisis en tiempo real y garantiza una gran transparencia. Más información sobre la *seguridad de la cadena de suministro de Axis*.
- Seguridad integrada de los dispositivos a través de Axis Edge Vault, que protege la integridad de los dispositivos Axis mediante las siguientes funciones:
  - **Sistema operativo firmado**: garantiza que el AXIS OS instalado es realmente de Axis. También comprueba que cualquier nuevo AXIS OS que deba instalarse en el dispositivo esté también firmado por Axis.
  - **Arranque seguro**: Permite al dispositivo comprobar que el sistema operativo tiene una firma de Axis. Si el sistema operativo no tiene autorización o se ha modificado, se cancela el proceso de arranque y el dispositivo deja de funcionar. La combinación de un sistema operativo firmado, un

arranque seguro y el restablecimiento de fábrica del dispositivo ofrece protección frente a intentos de modificación durante el envío de un dispositivo.

- El **ID de dispositivo Axis** es conforme con IEEE 802.1AR, lo que abre la puerta a la identificación segura del dispositivo y su incorporación a una red. El ID de dispositivo Axis se guarda en el almacén seguro de claves del dispositivo (elemento seguro, TPM, TEE).
- El **sistema de archivos cifrado** impide la extracción o la manipulación de configuraciones específicas de clientes o información almacenada en el sistema de archivos mientras el dispositivo no se utiliza, por ejemplo durante su transporte de un integrador de sistemas a un cliente.
- Además, gracias al **vídeo firmado** los usuarios que visionan las imágenes pueden verificar si el vídeo exportado desde un dispositivo ha sido manipulado o no. Esta prestación resulta especialmente útil en investigaciones o en procesos judiciales. Más información en *axis.com/solutions/edge-vault*.

- Se genera una suma de comprobación para las descargas de software realizadas desde axis.com. La suma de comprobación permite verificar la integridad de un archivo.
- Certificación ETSI: Más de 150 productos de Axis con AXIS OS 11 o superior tienen la certificación de conformidad con la *norma de ciberseguridad ETSI EN 303 645*. ETSI son las siglas en inglés correspondientes a Instituto Europeo de Normas de Telecomunicaciones. Estos requisitos hacen referencia a aspectos relacionados con los propios dispositivos, como la compatibilidad con funciones de seguridad integradas en el hardware como el almacenamiento seguro de claves y funciones de seguridad por omisión como HTTPS activado de forma predeterminada y la ausencia de contraseñas predeterminadas. Otra cuestión analizada es la gestión del ciclo de vida, como tener un periodo de soporte definido para las actualizaciones de seguridad de los dispositivos. También comprende requisitos como contar con una metodología para reducir el riesgo de vulnerabilidades en el desarrollo de software, tener una política transparente para la gestión de vulnerabilidades e implementar las prácticas recomendadas en el tratamiento de los datos personales. Estos requisitos tienen en cuenta las prácticas recomendadas en el sector, garantía de que los productos certificados tienen nivel de seguridad mínimo a lo largo de su ciclo de vida. La norma se ajusta estrechamente a la Ley de Ciberresiliencia de la UE, la Directiva sobre equipos radioeléctricos de la UE y otras normas y legislaciones internacionales.

4.8 Formación y orientación

Axis proporciona a su personal, socios y clientes información y formación sobre las prácticas recomendadas en el ámbito de la ciberseguridad. Aquí incluimos algunos:

- Sensibilización y formación en materia de seguridad interna: Axis ha desarrollado un programa de sensibilización sobre seguridad para ofrecer una formación continua a sus empleados con el objetivo de evitar y mitigar las amenazas a la seguridad para la organización. Esta formación sobre sensibilización es obligatoria para todo el personal de Axis. Dependiendo de las funciones y responsabilidades organizativas de cada persona, se ofrece formación adicional sobre seguridad a los desarrolladores y responsables de sistemas.
- *Formación en Axis Academy*: Entre los cursos de formación disponibles para los clientes hay un curso online sobre ciberseguridad y la *estrategia de Axis en este tema*.
- *Guías de seguridad* disponibles online para:
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Switches de red Axis*

- *Guía de análisis de seguridad de AXIS OS*: Axis recomienda realizar análisis de seguridad de sus dispositivos para comprobar si presentan vulnerabilidades o una configuración deficiente. La Guía de análisis de seguridad de AXIS OS incluye recomendaciones para resolver algunos de los avisos de los análisis y presenta los falsos positivos más habituales.
- *Guía forense de AXIS OS*: Esta guía incluye recomendaciones técnicas para realizar análisis forenses de dispositivos Axis en caso de ciberataque en la red y la infraestructura de TI en las que está instalado un dispositivo Axis.

Para obtener más información sobre Axis y la ciberseguridad, visite el *portal de ciberseguridad de Axis.*

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones para mejorar la seguridad y el rendimiento empresarial. Como empresa de tecnología de red y líder del sector, Axis ofrece soluciones de videovigilancia, control de acceso y sistemas de audio e intercomunicación. Se ven reforzadas por aplicaciones de análisis inteligentes y respaldadas por formación de alta calidad.

Axis tiene alrededor de 4000 empleados dedicados en más de 50 países y colabora con socios de integración de sistemas y tecnología en todo el mundo para ofrece soluciones personalizadas. Axis se fundó en 1984 y la sede está en Lund, Suecia

©2024 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC y VAPIX son marcas comerciales registradas de Axis AB en distintas jurisdicciones. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios. Nos reservamos el derecho a introducir modificaciones sin previo aviso.