GRUNDIG

Guía de cumplimiento de la NIS2 de GRUNDIG Security

Revisión 05/2026

Prólogo

La Directiva NIS2 de la Unión Europea[1] endurece drásticamente los requisitos de ciberseguridad para las infraestructuras críticas y sus cadenas de suministro. **GRUNDIG** Security, como fabricante certificado según las normas ISO 9001 e ISO 27001, ofrece soluciones de tecnología de vídeo a medida y conformes con la legislación para cumplir de manera eficiente estos estrictos requisitos legales.

Antecedentes de la normativa

Desde enero de 2023, la Directiva NIS2 está en vigor a nivel de la UE con el fin de armonizar de manera coherente el nivel general de seguridad de las redes y los sistemas de información. La transposición nacional amplía el número de empresas afectadas en Alemania de las 4.500 actuales a unas 29.500 organizaciones. Esta ampliación masiva obliga a sectores económicos enteros a una reorientación fundamental de sus estrategias de TI.

Los años 2025 y 2026 exigirán a las empresas europeas un aumento drástico de su ciberresiliencia debido a una situación de seguridad geopolítica volátil. La nueva Directiva NIS2 aborda las deficiencias del mercado en materia de seguridad informática mediante requisitos normativos de gran alcance y estrictos. Como fabricante de tecnología de vídeo, **GRUNDIG** Security apoya activamente a los planificadores, instaladores y operadores afectados para garantizar la seguridad exigida en la cadena de suministro.

Objetivos principales de la Directiva

NIS2 tiene como objetivo reforzar de manera significativa la capacidad de defensa de toda la economía europea frente a amenazas digitales y físicas. Para ello, la ley establece criterios más estrictos en materia de gestión de riesgos cibernéticos, continuidad de las operaciones y gestión de vulnerabilidades. Además, el concepto de protección se amplía de forma vinculante más allá de los límites de la empresa, abarcando a proveedores y prestadores de servicios.

Importancia para la tecnología de vídeo en general

Los sistemas modernos de videovigilancia están altamente interconectados y profundamente integrados en los complejos entornos de TI y TO de los operadores. Por ello, se consideran relevantes para la seguridad y representan una puerta de entrada potencial para ciberataques graves.

Clasificación de las instalaciones

La Directiva NIS2 clasifica a las organizaciones afectadas en dos categorías principales en función de su criticidad. Las diferencias se manifiestan principalmente en el tamaño de la empresa, la supervisión administrativa y el marco sancionador legal.

Clasificación: Entidades esenciales

Entre las instalaciones esenciales se incluyen las grandes empresas de sectores altamente críticos, como la energía, el transporte, la banca, la sanidad y la infraestructura digital. Los operadores de instalaciones críticas clásicas (KRITIS) entran automáticamente en esta categoría regulatoria más alta. Estas organizaciones están sujetas a la supervisión administrativa más estricta y deben demostrar los más altos estándares de resiliencia.

[1] Fuente: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2

Clasificación: Instalaciones importantes

La categoría de instalaciones importantes abarca empresas medianas y grandes de sectores como la gestión de residuos, la producción alimentaria, la industria manufacturera y la industria química. Se considera que una empresa es mediana si cuenta con más de 50 empleados o genera una facturación superior a 10 millones de euros. Aunque la supervisión en este caso es reactiva, los requisitos básicos de seguridad para estas empresas son idénticos.

Característica	Instalaciones esenciales	Instalaciones importantes
Sector de pertenencia	Altamente críticas (p. ej., KRITIS, energía)	Otros críticos (p. ej., alimentación)
Tamaño de la empresa	Grandes empresas (>250 empleados)	Medianas y grandes empresas (>50 empleados)
Tipo de supervisión	Estricta y proactiva	Reactivo (en función de las circunstancias)
Multa máxima	10 millones de euros o el 2 % de la facturación global	7 millones de euros o el 1,4 % de la facturación global

Identificación y registro

Las empresas tienen la obligación de comprobar por sí mismas si se ven afectadas por la Directiva NIS2 e identificarlas de conformidad con la ley. Las organizaciones afectadas deben registrarse obligatoriamente ante la autoridad nacional competente, como la BSI en Alemania. Es obligatorio designar ante la autoridad un punto de contacto central para la gestión de la seguridad de la información.

Los instaladores y los proyectistas deben garantizar el cumplimiento de forma conjunta.

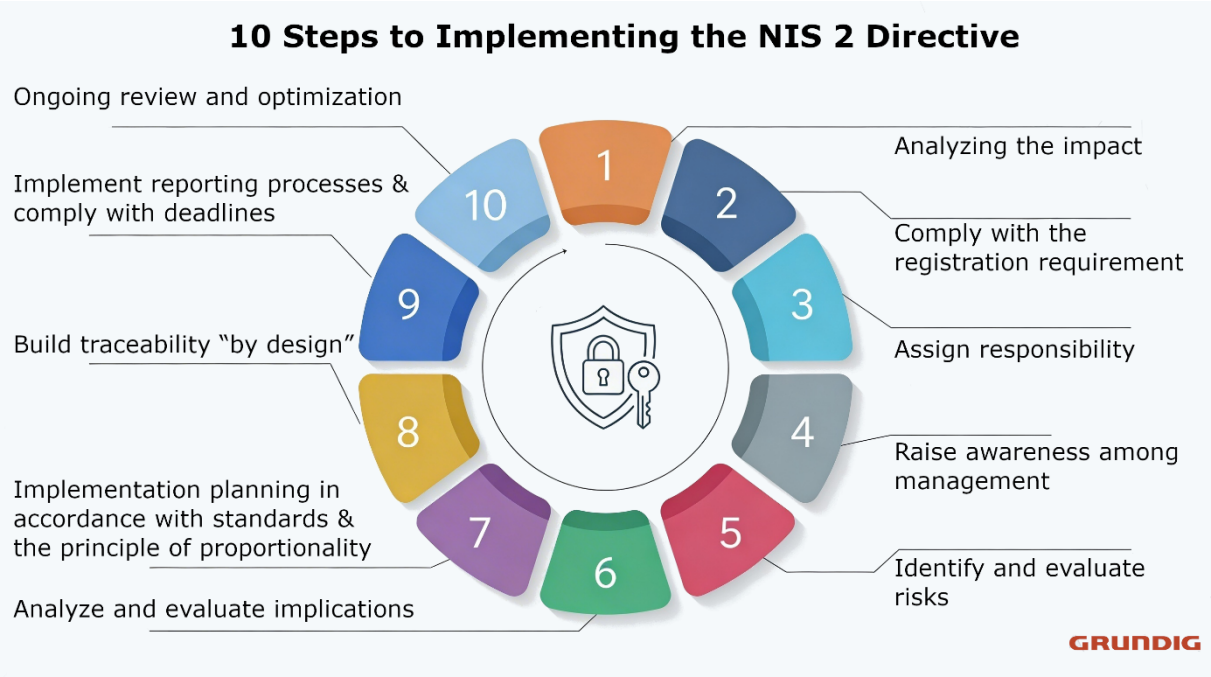
Estrictas obligaciones de notificación

En caso de incidentes de seguridad graves, las entidades deben enviar una alerta temprana oficial a la autoridad supervisora en un plazo de 24 horas. La legislación exige un informe detallado y exhaustivo del incidente en un plazo máximo de 72 horas. Además, en el plazo de un mes, la autoridad puede solicitar un informe final detallado sobre las causas y las medidas correctivas adoptadas.

Las empresas reguladas deben demostrar en todo momento una gran disposición a cooperar con los organismos de control estatales. Esto incluye el suministro fluido de información y el acceso temporal a los sistemas informáticos para las investigaciones de las autoridades. La cooperación proactiva es fundamental en este sentido para evitar rápidamente riesgos sistémicos para la comunidad.

Obligaciones de documentación

Todas las medidas de seguridad y los procesos operativos implementados deben documentarse de forma completa y comprensible. La eficacia de estas pruebas debe verificarse mediante auditorías periódicas e independientes. A petición de las autoridades, estos documentos estructurados deben poder presentarse en cualquier momento dentro de los plazos establecidos.



Medidas de ciberseguridad

La ley exige medidas técnicas, operativas y organizativas adecuadas para minimizar los riesgos cibernéticos de gran alcance. Entre ellas se incluyen estrategias de copia de seguridad exhaustivas, procedimientos de recuperación ante desastres y una gestión sistemática de la respuesta a incidentes. También se prescribe explícitamente el uso de comunicaciones seguras de voz, vídeo y texto en áreas sensibles.

Ciberseguridad exigida

Las entidades deben aplicar rigurosamente prácticas básicas de ciberhigiene para minimizar las vulnerabilidades. Esto incluye formación obligatoria para los empleados, controles de acceso estrictos y una gestión de activos mantenida de forma sistemática. Además, es obligatorio establecer autenticaciones multifactoriales para todos los accesos a sistemas críticos.

Sanciones inminentes y responsabilidad de la dirección del cliente final

En caso de «incumplimiento», las entidades de importancia crítica se enfrentan a multas drásticas de hasta 10 millones de euros o el 2 % de su facturación anual mundial. Para las entidades importantes, el límite máximo es de 7 millones de euros o el 1,4 % de la facturación global. Estas enormes sanciones tienen por objeto ejercer un efecto disuasorio y obligar a las empresas a dar prioridad a la seguridad informática.

Gracias a la NIS2, la ciberseguridad pasa a ocupar estratégicamente el nivel directivo más alto y se declara definitivamente una cuestión de máxima prioridad. En el futuro, los directores generales y los miembros del consejo de administración serán personalmente responsables del incumplimiento de las obligaciones legales en caso de infracciones u omisiones. Además, la ley prevé cursos de formación en seguridad obligatorios y periódicos para toda la dirección.

Riesgos en caso de incumplimiento

Los fabricantes que no cuenten con procesos de ciberseguridad demostrables serán excluidos sistemáticamente de las cadenas de suministro de las entidades reguladas por NIS2. Además, en caso de incidentes de seguridad, pueden ser sancionados económicamente por responsabilidad por

productos defectuosos y elevadas reclamaciones de indemnización. Los riesgos geopolíticos y la ausencia en las listas de confianza internacionales también conducen a la exclusión directa del mercado.

GRUNDIG Security como socio

GRUNDIG Security, como socio europeo de confianza, ofrece apoyo a medida para el cumplimiento de la NIS2 a sus clientes profesionales. Combinamos hardware de alto rendimiento con el flexible software de gestión de vídeo C-WERK para crear un sistema global de alta seguridad. Este enfoque integrador supone un gran alivio para los operadores de instalaciones a la hora de cumplir con sus obligaciones en la cadena de suministro.

Estado de la técnica

La Directiva NIS2 exige que los dispositivos informáticos se ajusten al estado actual de la técnica. Esto incluye, por supuesto, el uso de cámaras, grabadoras y servidores.

Las cámaras, los grabadores y los servidores son objetivos habituales de los ciberataques. Ya sea para espiar comportamientos o para crear una denominada red de bots, el acceso al firmware y al software de la tecnología de seguridad resulta muy valioso desde el punto de vista de un atacante.

En lo que respecta a la ciberseguridad, las versiones de firmware de nuestras líneas de productos están reforzadas, se han sometido a pruebas contra diversos vectores de ataque y se auditan internamente de forma permanente.

IA y análisis de vídeo

El estado de la técnica exigido en la tecnología de vídeo requiere cada vez más el uso de la inteligencia artificial para la detección automatizada de amenazas. La línea SMART de **GRUNDIG** Security procesa análisis como el reconocimiento facial, la vigilancia perimetral y el «virtual tripwire» de conformidad con la normativa de protección de datos directamente en la cámara, el grabador o el servidor.

Seguridad desde el diseño

Según el artículo 21 de la Directiva NIS2, los productos de TI deben diseñarse siguiendo estrictos principios de seguridad ya desde la primera fase de desarrollo. **GRUNDIG** Security integra de forma sistemática esta filosofía de «seguridad desde el diseño» en el sistema de gestión de vídeo C-WERK y en todas las cámaras de red que ofrece. Los sistemas de vigilancia se entregan a los clientes finales de serie con ajustes preestablecidos seguros (Security by Default) y una superficie de ataque minimizada.

Las innovadoras funciones de la línea SMART, como «One-Click-Disable», bloquean cualquier comunicación con Internet cuando es necesario, incluso si los dispositivos reciben una puerta de enlace válida para conectarse.

Nube y cifrado

Una transmisión de datos segura en todo momento es un requisito fundamental de las obligaciones de gestión de riesgos de la NIS2. **GRUNDIG** Security permite una comunicación fluida y altamente cifrada entre el hardware local y la nube C-WERK conectada. Esta arquitectura protege de forma fiable los metadatos sensibles contra el acceso de terceros no autorizados y garantiza la seguridad jurídica de los proyectos de vigilancia que abarcan varias ubicaciones.

Enfoque en la seguridad de la cadena de suministro

Un elemento central de la Directiva NIS2 es la protección sistemática de toda la cadena de suministro, de conformidad con el artículo 21. Las entidades afectadas deben supervisar y auditar estrictamente la ciberseguridad de sus proveedores y prestadores de servicios. En última instancia, la cadena de seguridad de una organización es tan resistente como su proveedor externo más débil.

Procesos de seguridad certificados

La respuesta más fiable a las obligaciones de acreditación de la NIS2 en la cadena de suministro son las certificaciones independientes e internacionales. **GRUNDIG** Security cuenta con las exigentes certificaciones ISO 9001 para la gestión de la calidad e ISO 27001 para la gestión de la seguridad de la información. Estos sellos de calidad oficiales garantizan a los clientes que todos los procesos de desarrollo y empresariales están sujetos a los más altos estándares de seguridad y son auditados sistemáticamente por terceros.

Conformidad y confianza

La independencia geopolítica absoluta es un criterio decisivo para la selección de proveedores de tecnología de confianza bajo el régimen NIS2. Por lo tanto, todas las cámaras y grabadoras de la línea SMART de **GRUNDIG** Security cumplen plenamente con los estrictos estándares de la NDAA. Esto excluye los componentes críticos de proveedores de alto riesgo y garantiza la soberanía digital de las infraestructuras críticas europeas.

Además, nuestras cámaras y grabadoras Smart-Line cumplen con las directrices de la denominada «NDAA compliance». Esta normativa prohíbe a las autoridades estadounidenses y a sus contratistas el uso de tecnología de telecomunicaciones y videovigilancia de determinados fabricantes chinos, con el fin de minimizar los riesgos de seguridad.

Gestión de vulnerabilidades

Una gestión ágil y proactiva de las vulnerabilidades es un requisito legal obligatorio para las instalaciones críticas. **GRUNDIG** Security apoya a sus clientes finales en este sentido mediante actualizaciones continuas de firmware y la distribución extremadamente rápida de parches de seguridad. La estricta compatibilidad con estándares abiertos como ONVIF garantiza además que los sistemas sigan siendo compatibles a largo plazo con otros fabricantes.

GRUNDIG Security participa, junto con su socio tecnológico Axxonsoft, en el programa «Common Vulnerabilities and Exposures (CVE)» de la MITRE Corporation. Este sistema estandarizado para la identificación y catalogación de vulnerabilidades de ciberseguridad de dominio público en software y hardware permite la publicación y el seguimiento de vectores de ataque.

Más información en el siguiente enlace:
https://www.cve.org/PartnerInformation/ListofPartners/partner/AxxonSoft

Autenticación de red

La legislación europea exige controles de acceso estrictos y el uso de métodos criptográficos robustos para proteger las redes de las instalaciones. Las grabadoras y cámaras IP de **GRUNDIG** Security admiten entradas de alarma complejas, así como los mecanismos de autenticación más modernos según los estándares IEEE. De este modo, todos los productos de la línea Smart-Line admiten el control de acceso a la red basado en puertos (PNAC) según IEEE 802.1X.

El VMS C-WERK ofrece, además, una gestión de derechos con seguridad forense que excluye técnicamente por completo cualquier manipulación no autorizada de los datos.

Conclusión

Los operadores de sistemas de videovigilancia deben asegurarse de que su infraestructura de TI pueda cumplir sin problemas con las futuras regulaciones. La integración perfecta de las tecnologías IP y HD-TVI en la cartera de **GRUNDIG** Security permite una migración escalable y con seguridad de inversión de los sistemas existentes. Esto garantiza una implementación económicamente razonable y, al mismo tiempo, totalmente conforme a la ley de las medidas técnicas requeridas.

Gracias a la colaboración exclusiva con un fabricante certificado según la norma ISO 27001 como **GRUNDIG** Security, las empresas críticas reducen enormemente su propio riesgo de incumplimiento normativo. La documentación exhaustiva y la certificación de productos de seguridad probada protegen de forma fiable a las instalaciones frente a sanciones estatales que pueden ascender a millones de euros. Al mismo tiempo, este enfoque libera en gran medida a la dirección de la empresa de riesgos de responsabilidad personal que podrían poner en peligro su existencia.

www.grundig-security.com

Abetechs GmbH (**GRUNDIG** Security)

info@grundig-security.com

Sujeto a cambios y errores.

GRUNDIG