GRUNDIG

Guida alla conformità NIS2 di GRUNDIG Security

Revisione 05/2026

Prefazione

La direttiva NIS2 dell'Unione Europea[1] inasprisce drasticamente i requisiti di sicurezza informatica per le infrastrutture critiche e le loro catene di fornitura. In qualità di produttore certificato ISO 9001 e ISO 27001, **GRUNDIG** Security offre soluzioni di videosorveglianza su misura e conformi alla normativa, per soddisfare in modo efficiente questi severi requisiti di legge.

Contesto normativo

Da gennaio 2023 la direttiva NIS2 è in vigore a livello UE per armonizzare in modo coerente il livello generale di sicurezza delle reti e dei sistemi informativi. L'attuazione a livello nazionale amplia la cerchia delle aziende interessate in Germania da 4.500 a circa 29.500 organizzazioni. Questo massiccio ampliamento costringe interi settori economici a un radicale riorientamento delle loro strategie IT.

Gli anni 2025 e 2026 richiedono alle aziende europee un drastico aumento della loro resilienza informatica a causa di una situazione di sicurezza geopolitica instabile. La nuova direttiva NIS2 affronta le carenze del mercato in materia di sicurezza informatica attraverso requisiti normativi di ampia portata e rigorosi. In qualità di produttore di tecnologia video, **GRUNDIG** Security supporta attivamente i progettisti, gli installatori e gli operatori interessati nel garantire la sicurezza richiesta nella catena di fornitura.

Obiettivi principali della direttiva

NIS2 mira a rafforzare in modo massiccio la capacità di difesa dell'intera economia europea contro le minacce digitali e fisiche. A tal fine, la legge applica standard più severi alla gestione dei rischi informatici, alla continuità operativa e alla gestione delle vulnerabilità. Inoltre, il concetto di protezione viene esteso in modo vincolante oltre i confini aziendali a fornitori e prestatori di servizi.

Significato per la tecnologia video in generale

I moderni sistemi di videosorveglianza sono altamente interconnessi e profondamente integrati nei complessi ambienti IT e OT degli operatori. Di conseguenza, sono considerati rilevanti per la sicurezza e rappresentano una potenziale porta d'accesso per gravi attacchi informatici.

Classificazione delle strutture

La direttiva NIS2 classifica le organizzazioni interessate in due categorie principali, essenziali e importanti, in base alla loro criticità. Le differenze si manifestano principalmente nelle dimensioni dell'azienda, nella supervisione delle autorità e nel quadro sanzionatorio previsto dalla legge.

NIS2 in Italia

In Italia, la direttiva NIS2 classifica le strutture in Soggetti Essenziali e Soggetti Importanti basandosi su settore di attività e dimensione (dipendenti o M€ fatturato). I soggetti essenziali (es. energia, trasporti, sanità) hanno obblighi più stringenti rispetto a quelli importanti, con vigilanza reattiva o proattiva. Di seguito i dettagli della classificazione NIS2 in Italia:

Classificazione: Soggetti essenziali

Germania

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

Tra le infrastrutture essenziali figurano le grandi imprese dei settori altamente critici quali energia, trasporti, settore bancario, sanità e infrastrutture digitali. Queste organizzazioni sono soggette alla più rigorosa vigilanza delle autorità e devono dimostrare i più elevati standard di resilienza.

Gli operatori di impianti critici classici (KRITIS) rientrano automaticamente in questa classe di regolamentazione più elevata.

Italia

Include energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi TIC, pubblica amministrazione (centrale PAC e locale PAL), e aerospazio.

L'equivalente italiano di KRITIS (*Kritische Infrastrukturen*) è Infrastrutture Critiche (IC), classificate dall'Agenzia Italiana ACN (acn.gov.it) attraverso il CSIRT (*Computer Security Incident Response Team*). Si tratta di team specializzati, operativi a livello nazionale o aziendale, incaricati di prevenire, gestire e rispondere agli incidenti di sicurezza informatica.

Soggetti importanti

Germania

La categoria delle strutture importanti comprende le medie e grandi imprese di settori quali la gestione dei rifiuti, la produzione alimentare, l'industria manifatturiera e l'industria chimica. Le imprese sono considerate di medie dimensioni se impiegano più di 50 dipendenti o generano un fatturato superiore a 10 milioni di euro. Sebbene la vigilanza in questo caso sia di tipo reattivo, i requisiti di sicurezza di base per queste aziende sono identici.

Italia

Copre altri settori critici come servizi postali, gestione dei rifiuti, fabbricazione/distribuzione di prodotti chimici, produzione/trasformazione/distribuzione di alimenti, fabbricazione di dispositivi medici, apparecchiature elettroniche e autoveicoli, fornitori digitali (non essenziali) e ricerca.

Riepilogo strutture

Caratteristica	Soggetti essenziali	Soggetti importanti
Appartenenza settoriale	Altamente critiche (ad es. IC, energia)	Altri settori critici (ad es. alimentare)
Dimensioni dell'azienda	Grandi imprese (dipendenti >250 ovvero fatturato >50M€)	Medie e grandi imprese (dipendenti >50 ovvero fatturato >10M€)
Tipo di vigilanza	Rigorosa e proattiva	Reattivo (in base alle circostanze)
Obblighi di segnalazione	Devono adottare misure di cybersicurezza e notificare incidenti a CSIRT	Devono adottare misure di cybersicurezza e notificare incidenti a CSIRT

Caratteristica	Soggetti essenziali	Soggetti importanti
Sanzione massima	10 milioni di euro o il 2% del fatturato globale	7 milioni di euro o l'1,4% del fatturato globale

Identificazione e registrazione

Le aziende hanno l'obbligo di verificare autonomamente la propria soggezione alla direttiva NIS2 e di identificarla in conformità con la legge. Le organizzazioni interessate devono obbligatoriamente registrarsi presso l'autorità nazionale competente, come il BSI in Germania ovvero l'ACN in Italia. È obbligatorio designare un punto di contatto centrale per la gestione della sicurezza delle informazioni nei confronti dell'autorità.

I progettisti e i costruttori devono garantire l'adempimento in collaborazione.

Rigorosi obblighi di segnalazione

In caso di incidenti di sicurezza significativi, le strutture devono inviare un allarme preventivo ufficiale all'autorità di vigilanza entro 24 ore. Il legislatore richiede una segnalazione dettagliata ed esaustiva dell'incidente entro e non oltre 72 ore. Entro un mese, l'autorità può inoltre richiedere una relazione finale dettagliata sulle cause e sulle contromisure adottate.

Le imprese regolamentate devono dimostrare in ogni momento un'elevata disponibilità alla cooperazione nei confronti degli organismi di controllo statali. Ciò comprende la fornitura senza intoppi di informazioni e l'accesso temporaneo ai sistemi informatici per le indagini delle autorità. Una collaborazione proattiva è fondamentale in questo contesto per scongiurare rapidamente i pericoli sistemici per la collettività.

Obblighi di documentazione

Tutte le misure di sicurezza e i processi operativi implementati devono essere documentati in modo completo e tracciabile. L'efficacia di tali prove deve essere verificata tramite audit regolari e indipendenti. Su richiesta delle autorità, questi documenti strutturati devono poter essere presentati in qualsiasi momento entro i termini previsti.

Il quadro normativo di riferimento in Italia

La Direttiva (UE) 2022/2555 è stata recepita nell'ordinamento italiano con il D.Lgs. 4 settembre 2024, n. 138, entrato in vigore il 16 ottobre 2024. Il decreto estende gli obblighi di sicurezza informatica a 18 settori critici: dall'energia alla sanità, dai trasporti alle infrastrutture digitali, coinvolgendo tanto i soggetti privati quanto le pubbliche amministrazioni classificati come essenziali o importanti.

Il quadro degli obblighi operativi è stato definitivamente consolidato a fine dicembre 2025 con l'adozione di due determinazioni del Direttore Generale dell'ACN:

- Determinazione ACN n. 379887/2025, che disciplina il Portale NIS (registrazioni, aggiornamento informazioni, designazioni), applicabile dal 31 dicembre 2025.
- Determinazione ACN n. 379907/2025, che definisce le misure di sicurezza di base e gli incidenti significativi di base, applicabile dal 15 gennaio 2026.

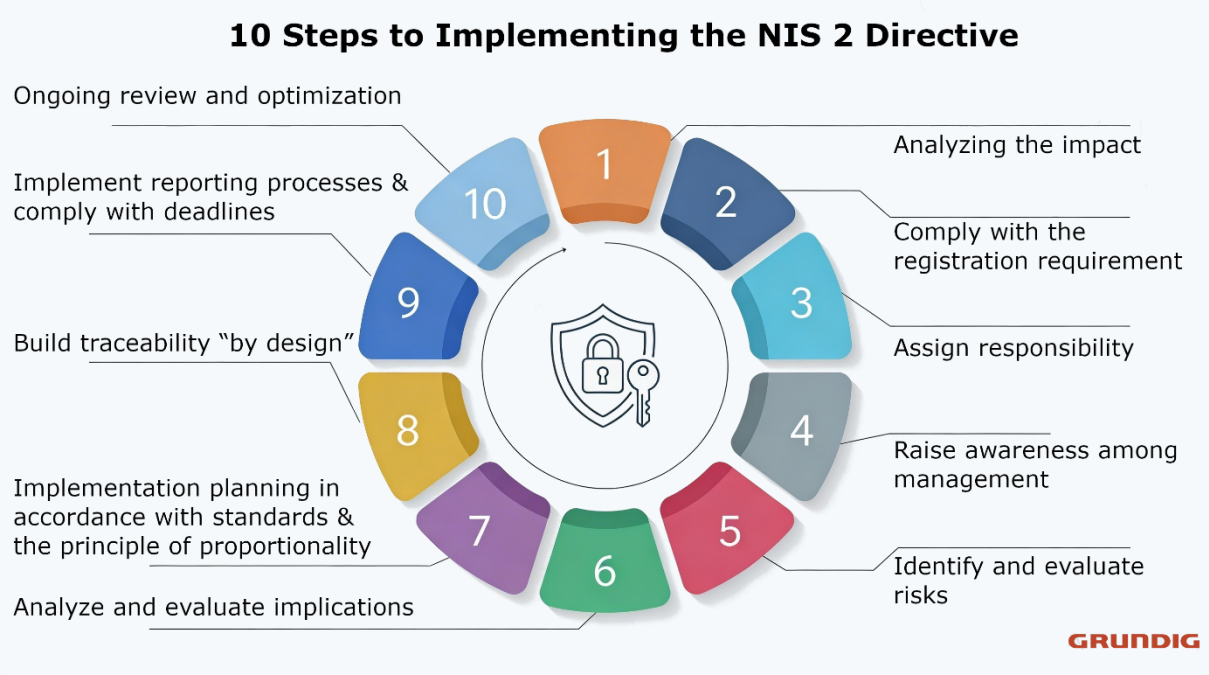
A queste si affianca il Regolamento di esecuzione (UE) 2024/2690, che specifica requisiti tecnici e metodologici per categorie specifiche di fornitori digitali, tra cui DNS, cloud, data center, CDN, marketplace, piattaforme social e prestatori di servizi fiduciari.

La struttura degli obblighi in Italia

Prima di entrare nel dettaglio delle scadenze, è necessario comprendere l'architettura degli obblighi così come definita dal Decreto e dalla pagina normativa ufficiale dell'ACN. Gli adempimenti si articolano su due filoni principali, entrambi con termini che decorrono dalla comunicazione di inserimento nell'elenco nazionale NIS inviata dall'ACN ai soggetti individuati tra marzo e aprile 2025:

- **9 mesi dalla comunicazione**: obbligo di notifica degli incidenti significativi al CSIRT Italia, con scadenza al 15 gennaio 2026.
- **18 mesi dalla comunicazione**: adozione delle misure di sicurezza di base, con scadenza entro ottobre 2026.

Come precisa la sezione "Modalità e specifiche di base" del portale ACN, i soggetti importanti adottano le misure dell'Allegato 1, i soggetti essenziali quelle dell'Allegato 2 della Determinazione 379907/2025. Non si tratta di date universali fisse, ma di termini mobili: chi ha ricevuto la comunicazione ACN ad aprile 2025 ha come scadenza ottobre 2026; chi la ricevesse in ritardo avrà un termine corrispondentemente protratto.



Misure di sicurezza informatica

La legge richiede misure tecniche, operative e organizzative adeguate a ridurre al minimo i rischi informatici di ampia portata. Queste includono strategie di backup complete, procedure di *Disaster Recovery* e una gestione sistematica della risposta agli incidenti. Anche l'uso di comunicazioni vocali, video e testuali sicure è esplicitamente prescritto in settori sensibili.

Cyber-igiene (igiene informatica) richiesta

Le strutture devono applicare rigorosamente le pratiche fondamentali di igiene informatica per ridurre al minimo le vulnerabilità. Ciò comprende corsi di formazione obbligatori per i dipendenti,

severi controlli di accesso e una gestione delle risorse costantemente aggiornata. Inoltre, è obbligatorio stabilire autenticazioni a più fattori per tutti gli accessi ai sistemi critici.

Sanzioni imminenti e responsabilità della direzione del cliente finale

In caso di cosiddetta «non conformità», le entità significative rischiano sanzioni drastiche fino a 10 milioni di euro o al 2% del fatturato annuo globale. Per le entità importanti, il limite massimo è fissato a 7 milioni di euro o all'1,4% del fatturato globale. Queste sanzioni enormi hanno lo scopo di esercitare un effetto deterrente e di imporre alle aziende di dare priorità alla sicurezza informatica.

Grazie alla NIS2, la sicurezza informatica assume un ruolo strategico al massimo livello dirigenziale e viene definitivamente dichiarata una questione di primaria importanza. In caso di violazioni o omissioni, gli amministratori delegati e i membri del consiglio di amministrazione saranno in futuro personalmente responsabili del mancato rispetto degli obblighi di legge. Inoltre, la legge prevede corsi di formazione obbligatori e regolari in materia di sicurezza per l'intera dirigenza.

Rischi in caso di inosservanza

I produttori sprovvisti di processi di sicurezza informatica dimostrabili saranno sistematicamente esclusi dalle catene di fornitura delle strutture regolamentate dalla NIS2. Inoltre, in caso di incidenti di sicurezza, potranno essere perseguiti finanziariamente in base alla responsabilità del produttore e a elevate richieste di risarcimento. Anche i rischi geopolitici e l'assenza da elenchi internazionali di fiducia comportano l'esclusione diretta dal mercato.

GRUNDIG Security come partner

GRUNDIG Security, in qualità di partner europeo affidabile, offre un supporto su misura per la conformità NIS2 dei propri clienti professionali. Combiniamo hardware potente con il software di gestione video flessibile C-WERK per creare un sistema completo altamente sicuro. Grazie a questo approccio integrativo, gli operatori degli impianti sono notevolmente alleggeriti nell'adempimento dei loro obblighi relativi alla catena di fornitura.

Stato dell'arte

La direttiva NIS2 richiede che i dispositivi IT siano conformi allo stato dell'arte. Ciò include naturalmente l'uso di telecamere, registratori e server.

Telecamere, registratori e server sono obiettivi molto ambiti dagli attacchi informatici. Che si tratti di spiare comportamenti o di creare una cosiddetta rete di bot, l'accesso al firmware e al software dei sistemi di sicurezza è molto redditizio dal punto di vista di un aggressore.

Per quanto riguarda la sicurezza informatica, le versioni del firmware delle nostre linee di prodotti sono rinforzate, testate contro diversi vettori di attacco e sottoposte a continui audit interni.

IA e analisi video

Lo stato dell'arte richiesto nella tecnologia video richiede sempre più l'uso dell'intelligenza artificiale per il rilevamento automatico delle minacce. La linea SMART di **GRUNDIG** Security elabora analisi come il riconoscimento facciale, la sorveglianza perimetrale e il *Virtual Tripwire* in conformità con la normativa sulla protezione dei dati direttamente sulla telecamera, sul registratore o sul server.

Security by Design

Ai sensi dell'articolo 21 della direttiva NIS2, i prodotti IT devono essere progettati secondo rigorosi principi di sicurezza già nella prima fase di sviluppo. **GRUNDIG** Security integra coerentemente questa filosofia di "Security by Design" nel sistema di gestione video C-WERK e in tutte le telecamere di rete

offerte. I sistemi di sorveglianza vengono forniti ai clienti finali di serie con impostazioni predefinite sicure (Security by Default) e con una superficie di attacco ridotta al minimo.

Funzioni innovative della linea SMART, come "One-Click-Disable", bloccano qualsiasi comunicazione con Internet quando serve, anche se i dispositivi ricevono un gateway valido per connettersi.

Cloud e crittografia

Una trasmissione dei dati sicura in ogni fase è un requisito fondamentale degli obblighi di gestione dei rischi previsti dalla direttiva NIS2. **GRUNDIG** Security consente una comunicazione fluida e altamente crittografata tra l'hardware locale e il cloud C-WERK collegato. Questa architettura protegge in modo affidabile i metadati sensibili dall'accesso di terzi non autorizzati e garantisce la conformità legale dei progetti di sorveglianza che coinvolgono più sedi.

Focus sulla sicurezza della catena di fornitura

Un elemento centrale della direttiva NIS2 è la protezione sistematica dell'intera catena di fornitura ai sensi dell'articolo 21. Le strutture interessate devono monitorare e verificare rigorosamente la sicurezza informatica dei propri fornitori e prestatori di servizi. La catena di sicurezza di un'organizzazione è, in definitiva, resistente solo quanto il suo fornitore terzo più debole.

Processi di sicurezza certificati

La risposta più affidabile agli obblighi di documentazione NIS2 nella catena di fornitura sono le certificazioni indipendenti e internazionali. **GRUNDIG** Security dispone delle rigorose certificazioni ISO 9001 per la gestione della qualità e ISO 27001 per la propria gestione della sicurezza delle informazioni. Questi marchi di qualità ufficiali garantiscono ai clienti che tutti i processi di sviluppo e aziendali sono soggetti ai più elevati standard di sicurezza e vengono sistematicamente sottoposti a audit da parte di terzi.

Conformità e fiducia

L'assoluta indipendenza geopolitica è un criterio decisivo per la selezione di fornitori di tecnologia affidabili nell'ambito del regime NIS2. Tutte le telecamere e i registratori della linea SMART di **GRUNDIG** Security sono quindi pienamente conformi ai rigorosi standard NDAA. Ciò esclude componenti critici provenienti da fornitori ad alto rischio e garantisce la sovranità digitale delle infrastrutture critiche europee.

Le nostre telecamere e i nostri registratori della linea Smart-Line soddisfano inoltre i requisiti di conformità al cosiddetto NDAA. Tale normativa vieta alle autorità statunitensi e ai loro appaltatori l'utilizzo di tecnologie di telecomunicazione e videosorveglianza prodotte da determinati produttori cinesi, al fine di ridurre al minimo i rischi per la sicurezza.

Gestione delle vulnerabilità

Una gestione agile e proattiva delle vulnerabilità è obbligatoria per legge per le strutture essenziali. **GRUNDIG** Security supporta i propri clienti finali in questo senso attraverso continui aggiornamenti del firmware e la distribuzione estremamente rapida di patch di sicurezza. La rigorosa compatibilità con standard aperti come ONVIF garantisce inoltre che i sistemi rimangano compatibili a lungo termine con produttori terzi.

GRUNDIG Security partecipa, insieme al partner tecnologico Axxonsoft, al programma "Common Vulnerabilities and Exposures (CVE)" della MITRE Corporation. Questo sistema standardizzato per l'identificazione e la catalogazione delle vulnerabilità di sicurezza informatica note al pubblico nel software e nell'hardware consente la pubblicazione e il monitoraggio dei vettori di attacco.

Maggiori informazioni al seguente link:
https://www.cve.org/PartnerInformation/ListofPartners/partner/AxxonSoft

Autenticazione di rete

La normativa europea richiede severi controlli di accesso e l'utilizzo di robusti metodi crittografici per la protezione delle reti degli impianti. I registratori e le telecamere IP **GRUNDIG** Security supportano ingressi di allarme complessi e meccanismi di autenticazione all'avanguardia secondo gli standard IEEE. Tutti i prodotti della linea Smart-Line supportano il controllo dell'accesso alla rete basato su porta (PNAC) secondo lo standard IEEE 802.1X.

Il VMS C-WERK offre parallelamente una gestione dei diritti protetta a livello forense, che esclude tecnicamente qualsiasi manipolazione non autorizzata dei dati.

Conclusione

I gestori di impianti video devono assolutamente garantire che la loro infrastruttura IT sia in grado di soddisfare senza problemi anche le normative future. La perfetta integrazione delle tecnologie IP e HD-TVI nel portafoglio di **GRUNDIG** Security consente una migrazione scalabile e sicura dal punto di vista degli investimenti degli impianti esistenti. Ciò garantisce un'attuazione economicamente proporzionata e tuttavia pienamente conforme alla legge delle misure tecniche richieste.

Grazie alla collaborazione esclusiva con un produttore certificato ISO 27001 come **GRUNDIG** Security, le aziende critiche riducono enormemente il proprio rischio di non conformità. La documentazione completa e la certificazione di prodotti comprovatamente sicuri proteggono in modo affidabile le strutture da sanzioni statali che possono ammontare a milioni di euro. Allo stesso tempo, questo approccio solleva in modo significativo la direzione aziendale da rischi di responsabilità personale che potrebbero mettere a repentaglio l'esistenza dell'azienda.