GUIDA PRATICA ALLA CONFORMITA'

NIS2

Cosa devi sapere e fare

Obblighi, soggetti coinvolti e sanzioni per le imprese italiane

IN SINTESI

La direttiva europea NIS2 e' legge. Le aziende che vi rientrano devono attivare misure concrete di sicurezza informatica.
Non e' un adempimento formale: la mancata conformita' espone a sanzioni economiche fino a milioni di euro.

INFOSECUR

Divisione Cybersecurity di IPKom Srl · www.infosecur.it

Che cos'e' la NIS2

Un obbligo di legge, non una scelta

La **NIS2** (Direttiva UE 2022/2555) e' la normativa europea che alza il livello minimo di sicurezza informatica per le organizzazioni che operano in settori considerati critici o importanti per il funzionamento della societa' e dell'economia. In Italia e' stata recepita con il **D.Lgs. 138/2024** ed e' pienamente in vigore.

Il punto centrale da comprendere e' questo: se la tua azienda rientra nel perimetro, **non hai discrezionalita'**. La legge ti impone di registrarti presso l'Agenzia per la Cybersicurezza Nazionale (ACN) e di adottare misure tecniche e organizzative precise. Non adeguarsi espone a sanzioni economiche e responsabilita' anche personali per gli organi di gestione.

> **Il concetto chiave**
>
> Adeguarsi alla NIS2 non e' un'operazione di facciata. Le aziende soggette **devono** attivare misure concrete di gestione del rischio cyber, perche' e' un preciso obbligo normativo — presidiato da un regime sanzionatorio.

Chi e' coinvolto

La normativa distingue due categorie di soggetti, in base al settore di attivita' e alla dimensione aziendale:

- **Soggetti essenziali** — operano in settori ad alta criticita' (energia, trasporti, sanita', acqua, infrastrutture digitali, PA, spazio) e superano le soglie dimensionali maggiori.
- **Soggetti importanti** — operano in settori critici (poste, rifiuti, chimica, alimentare, fabbricazione, servizi digitali) e superano soglie dimensionali intermedie.
- **Imprese collegate e catena di fornitura** — anche piccole imprese possono rientrare se forniscono servizi rilevanti a soggetti NIS o fanno parte di gruppi piu' grandi.

Attenzione: i codici ATECO sono solo indicativi. L'appartenenza al perimetro si determina sulle attivita' effettivamente svolte, tramite l'autovalutazione ufficiale sulla piattaforma ACN.

Gli obblighi da rispettare

Misure concrete, richieste dalla legge

I soggetti NIS2 devono adottare un insieme di misure tecniche, operative e organizzative proporzionate al rischio. Non sono facoltative: sono il contenuto minimo di conformita' richiesto dall'articolo 21 del decreto. Ecco le principali aree di intervento:

Analisi e gestione del rischio	Politiche di valutazione dei rischi e della sicurezza dei sistemi informativi.
Gestione degli incidenti	Procedure per prevenire, rilevare e rispondere agli incidenti di sicurezza.
Continuita' operativa	Backup, disaster recovery e gestione delle crisi per garantire i servizi.
Sicurezza della supply chain	Valutazione e presidio dei rischi legati a fornitori e partner.
Sicurezza nello sviluppo	Misure per acquisizione, sviluppo e manutenzione sicura dei sistemi.
Valutazione dell'efficacia	Verifica periodica dell'efficacia delle misure adottate.
Igiene informatica e formazione	Pratiche di base e formazione continua del personale.
Crittografia	Politiche e procedure sull'uso della crittografia dove appropriato.
Controllo degli accessi	Gestione delle identita' e degli accessi, autenticazione a piu' fattori.

Responsabilita' del management

La NIS2 coinvolge direttamente gli organi di amministrazione: devono approvare le misure, vigilare sulla loro attuazione e possono rispondere in caso di inadempimento. La sicurezza informatica diventa un tema di governance, non solo un problema tecnico.

Sanzioni e tempistiche

Perche' non si puo' rimandare

Il mancato rispetto degli obblighi NIS2 comporta sanzioni amministrative pecuniarie di importo significativo, differenziate tra soggetti essenziali e importanti:

Tipo di soggetto	Sanzione massima
Soggetti essenziali	Fino a **10 milioni €** o **2%** del fatturato annuo globale (il maggiore)
Soggetti importanti	Fino a **7 milioni €** o **1,4%** del fatturato annuo globale (il maggiore)
Mancata registrazione / comunicazione	Sanzioni amministrative fino allo **0,1%** del fatturato annuo globale

Oltre alle sanzioni economiche, sono previste misure accessorie che possono arrivare fino alla sospensione temporanea dei responsabili dalle funzioni dirigenziali.

Cosa fare, in pratica

- **Verifica** se la tua azienda rientra nel perimetro (settore + dimensione + ruolo nella supply chain).
- **Registrati** sulla piattaforma ACN tramite il Punto di Contatto con SPID e completa l'autovalutazione.
- **Nomina** i responsabili e attiva le misure di sicurezza richieste dall'art. 21.
- **Predisponi** le procedure di notifica degli incidenti (tempistiche 24h / 72h).
- **Mantieni** aggiornata la documentazione e la registrazione nel tempo.

Non sei solo in questo percorso

Infosecur affianca le aziende in ogni fase: dalla verifica dell'ambito di applicazione alla registrazione ACN, dall'analisi del rischio all'implementazione delle misure tecniche e organizzative richieste. Trasformiamo un obbligo complesso in un percorso gestito e sostenibile.

Vuoi sapere se la tua azienda e' soggetta alla NIS2?

Fai la verifica gratuita sul nostro sito o contattaci per una consulenza.

www.infosecur.it/nis2-check · commerciale@infosecur.it · +39 0575 1697500

Documento a scopo divulgativo, aggiornato alle disposizioni note. Non sostituisce la consulenza legale ne' la valutazione ufficiale dell'ambito di applicazione, che compete all'ACN. I riferimenti normativi principali sono la Direttiva UE 2022/2555 e il D.Lgs. 138/2024.