REGUVARA · GUIDA PRATICA GRATUITA

NIS2: preparare i canali di segnalazione e le evidenze

Un primo passo pratico per direzione, IT/sicurezza, legale e compliance. Orientamento su ambito, scadenze principali per le segnalazioni e cinque azioni iniziali.

Obiettivo: rendere rapidamente visibili le domande giuste. Questa guida non stabilisce in modo vincolante se una specifica entità giuridica rientra nell'ambito NIS2.

1. Valutare in via preliminare l'ambito

• Associare attività, servizio ed entità giuridica ai settori degli allegati I e II della direttiva NIS2. La sola denominazione del settore non determina l'inclusione.

• Verificare dimensioni, legami societari, tipo di servizio, eventuali designazioni critiche, esenzioni e regole dello Stato membro interessato. Alcune entità o servizi possono rientrare nell'ambito anche senza la soglia dimensionale ordinaria.

• Per ogni entità potenzialmente interessata, documentare paesi, sedi, servizi, autorità competente, obblighi di registrazione e contatto e motivazione.

2. Fasi di segnalazione UE per un incidente significativo

Fase	Quadro UE ai sensi dell'articolo 23	Domanda di preparazione
Preallarme	Senza ingiustificato ritardo e comunque entro 24 ore da quando si viene a conoscenza dell'incidente significativo.	Chi avvia il conteggio, decide e individua l'autorità competente?
Notifica dell'incidente	Senza ingiustificato ritardo e comunque entro 72 ore dalla conoscenza; prima valutazione di gravità e impatto e indicatori, se disponibili.	Come raccogliere in parallelo fatti, orari e aspetti ancora da chiarire?
Relazione intermedia	Se richiesta dal CSIRT o dall'autorità competente.	Chi registra gli aggiornamenti e risponde alle richieste?
Relazione finale	Di norma entro un mese dalla notifica dell'incidente. Se l'incidente è ancora in corso, a tale scadenza è dovuta una relazione sullo stato di avanzamento; la relazione finale va presentata entro un mese dalla gestione.	Chi conferma la scadenza nazionale e i contenuti richiesti?

Le scadenze riguardano gli incidenti significativi e il momento in cui se ne viene a conoscenza. Per i prestatori di servizi fiduciari si applica una regola speciale di 24 ore per la notifica dell'incidente. Verificare recepimento nazionale, norme settoriali e altri atti UE applicabili.

SCHEDA DI LAVORO

Dal testo normativo al primo processo operativo

NIS2 richiede misure tecniche, operative e organizzative proporzionate al rischio. Questa sintesi aiuta a riunire i primi responsabili.

3. Temi contemplati dall'articolo 21

Le misure proteggono le reti e i sistemi informativi usati per i servizi, compreso il loro ambiente fisico. Portata e progettazione dipendono dal rischio e dalla proporzionalità.

Area	Esempio di domanda operativa
Analisi dei rischi e sicurezza dei sistemi	Quali servizi, sistemi, minacce e dipendenze rientrano nella valutazione? Chi la aggiorna?
Gestione degli incidenti	Come sono organizzate rilevazione, classificazione, contenimento, escalation, conservazione delle prove e analisi successiva?
Continuità e crisi	Backup, ripristino, ruoli di crisi e obiettivi di ripresa sono documentati e testati?
Catena di fornitura	Sono registrati fornitori diretti, dipendenze critiche e informazioni di sicurezza?
Acquisto e sviluppo sicuri	Come si selezionano e mantengono i sistemi in modo sicuro e come si gestiscono o divulgano le vulnerabilità?
Verifica dell'efficacia	Come determina l'organizzazione se le misure di sicurezza funzionano?
Igiene informatica e formazione	Quali pratiche di base e formazioni sono pianificate e documentate?
Crittografia	Quali regole si applicano alla crittografia e, ove opportuno, alla cifratura?
Persone, accessi e risorse	Come vengono controllati autorizzazioni, cambi di personale, risorse e accessi?
Autenticazione e comunicazione	Dove sono appropriate MFA o autenticazione continua, comunicazioni sicure e canali di emergenza?

4. Cinque primi passi utili

- Designare una persona responsabile che coordini le questioni sull'ambito e i punti aperti.
- Inventariare servizi, entità giuridiche, sistemi e fornitori diretti critici.
- Nominare direzione, responsabile degli incidenti, IT/sicurezza, legale/compliance e comunicazione, con sostituti.
- Verificare autorità nazionale competente, CSIRT, registrazione, canale di segnalazione e obblighi settoriali.
- Svolgere una breve esercitazione: rilevare un incidente, registrare il momento della conoscenza, avviare l'escalation e costruire un quadro dei fatti.

NIS2 non si applica automaticamente a tutte le imprese. L'ambito dipende, tra l'altro, da attività, dimensioni, entità giuridica, Stato membro, casi particolari e regole settoriali.

FONTI E STATO GIURIDICO

Fonte primaria: direttiva (UE) 2022/2555, in particolare articoli 2-4, 20, 21 e 23 e allegati I-II. La proposta COM(2026) 13 final non è legge. L'8 ottobre 2026 la procedura 2026/0012(COD) del Parlamento europeo era in attesa di una decisione della commissione competente; il 24 settembre 2026 era stato pubblicato un progetto di relazione. Il recepimento nazionale e le norme settoriali non sono stati verificati paese per paese.
NIS2 Directive (EUR-Lex) · European Commission FAQ · National transposition · EP procedure 2026/0012(COD) · COM(2026) 13 proposal