PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6182 di Mercoledì 28 ottobre 2026

Scadenza NIS 2: entro il 31 ottobre 2026 l'adeguamento delle misure

Entro il 31 ottobre 2026 i soggetti NIS devono completare l'attuazione delle misure di sicurezza stabilite dall'ACN. Dal mese di novembre prenderanno il via le ispezioni formali per verificare la resilienza informatica e la continuità operativa.

Il panorama della cybersicurezza per le organizzazioni italiane entra in una fase cruciale. Il **31 ottobre 2026** rappresenta la scadenza perentoria stabilita dalla Determinazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) entro la quale i soggetti rientranti nel perimetro di applicazione del D.Lgs. 4 settembre 2024, n. 138 (di recepimento della Direttiva UE 2022/2555, nota come NIS 2) devono aver implementato e reso operative le misure di sicurezza informatica di base.

A partire dal mese di novembre 2026, l'ACN avvierà l'attività ispettiva formale per verificare la conformità dei sistemi e l'adeguatezza delle misure organizzative e tecniche adottate dai soggetti essenziali e importanti identificati nel corso del 2025.

Il quadro normativo: dal D.Lgs. 138/2024 alle determinazioni ACN

Il Decreto Legislativo n. 138/2024 ha ridefinito la governance nazionale della cybersicurezza, ampliando significativamente la platea dei soggetti tenuti a garantire elevati livelli di resilienza digitale. La normativa stabilisce obblighi chiari in materia di gestione dei rischi informatici e di notifica degli incidenti, ponendo in capo agli organi di amministrazione e direttivi una responsabilità diretta nell'approvazione e nella verifica delle misure di sicurezza.

La Determinazione dell'Agenzia per la Cybersicurezza Nazionale ha successivamente dettagliato la tempistica attuativa, fissando per il 31 ottobre 2026 il termine ultimo entro cui le aziende registrate nel perimetro NIS devono completare l'adozione degli standard minimi di sicurezza.

L'approccio normativo richiede il passaggio da un modello di gestione della sicurezza puramente reattivo a una struttura fondata sull'analisi del rischio e sulla continuità operativa.

Pubblicità

Le tre pilastri operativi in scadenza al 31 ottobre

Entro la data limite del 31 ottobre 2026, i soggetti obbligati devono dimostrare il completo recepimento di tre pilastri fondamentali per la gestione della cybersicurezza aziendale:

1. Analisi dei rischi e politiche di sicurezza delle informazioni

Le organizzazioni devono disporre di una governance formale della sicurezza informatica. Ciò comprende:

- La mappatura completa degli asset informatici, dei processi critici e delle interdipendenze tecnologiche.
- L'adozione di politiche formali per l'analisi dei rischi e la sicurezza dei sistemi informativi, in linea con i principali standard internazionali (es. ISO/IEC 27001).
- L'implementazione di procedure di controllo degli accessi, crittografia e autenticazione a più fattori (MFA).

2. Gestione degli incidenti e resilienza operativa (Incident Response)

La capacità di rilevare, analizzare e contenere tempestivamente un evento avverso è un requisito centrale della Direttiva NIS 2. Entro la scadenza prevista, è necessario disporre di:

- Piani di risposta agli incidenti informatici (*Incident Response Plan*) formalizzati e testati periodicamente.
- Procedure operative atte a garantire il rispetto delle tempistiche di notifica verso il CSIRT Italia (Computer Security Incident Response Team), che prevedono un pre-allarme entro 24 ore dalla conoscenza dell'incidente e una notifica completa entro 72 ore.
- Misure di backup e strategie di *Disaster Recovery* idonee a garantire il ripristino delle attività in caso di eventi bloccanti.

3. Sicurezza della catena di approvvigionamento (Supply Chain Security)

Il D.Lgs. 138/2024 richiede che la valutazione del rischio non si limiti al perimetro interno dell'azienda, ma si estenda all'intero ecosistema dei fornitori. I soggetti NIS devono:

- Valutare il livello di vulnerabilità e le prassi di sicurezza adottate da ciascun fornitore diretto di servizi e tecnologie ICT.
- Inserire clausole contrattuali vincolanti relative ai requisiti minimi di sicurezza e agli obblighi di comunicazione tempestiva di eventuali violazioni subite lungo la filiera.

Al via le ispezioni ACN da novembre 2026

Il rispetto del termine del 31 ottobre integra il presupposto per l'avvio della fase di vigilanza. A partire da novembre 2026, l'Agenzia per la Cybersicurezza Nazionale attiverà il piano di controlli e ispezioni formali sui soggetti essenziali e importanti.

Gli accertamenti dell'Autorità saranno volti a verificare:

- La presenza e l'effettiva applicabilità della documentazione di gestione del rischio e dei piani di risposta agli incidenti.
- L'adeguatezza tecnica delle soluzioni adottate per la protezione della rete e dei dati.
- Il grado di consapevolezza e formazione del personale, compresi i membri degli organi direttivi, in materia di sicurezza informatica.

Le sanzioni previste dal D.Lgs. 138/2024 per il mancato adempimento degli obblighi comprendono sanzioni amministrative pecuniarie di importo rilevante (fino a 10 milioni di euro o al 2% del fatturato annuo globale per i soggetti essenziali) e la possibilità di prescrizioni dirette volte al ripristino della conformità.

Indicazioni operative per le funzioni HSE e i Responsabili di Sicurezza

Sebbene la gestione della cybersicurezza attenga primariamente alla funzione IT e ai CISO, la convergenza tra sicurezza delle informazioni e sicurezza nei luoghi di lavoro (Safety) rende indispensabile il coinvolgimento attivo dei Responsabili del Servizio di Prevenzione e Protezione (RSPP) e degli HSE Manager.

Nelle realtà industriali e nelle infrastrutture critiche, la compromissione di un sistema OT (*Operational Technology*) o SCADA può comportare rischi diretti per la salute e la sicurezza dei lavoratori, determinando il malfunzionamento di dispositivi di

blocco, allarmi o linee produttive.

Si raccomanda pertanto alle funzioni aziendali di prevenzione di:

1. **Verificare l'integrazione del rischio cyber** all'interno del Documento di Valutazione dei Rischi (DVR) per gli impianti automatizzati o interconnessi.
2. **Coordinare i piani di emergenza** interni con i piani di *Incident Response* predisposti per la risposta agli attacchi informatici.
3. **Promuovere la formazione congiunta** del personale operativo sulle corrette prassi di utilizzo delle tecnologie aziendali e sulla segnalazione tempestiva delle anomali di sistema.

RXY

 Licenza Creative Commons
I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.
