31 gennaio 2026

lawalert

le ultime novità in tema di normative e giurisprudenza

Cybersecurity: Linee Guida NIS dell'Agenzia per la Cybersicurezza Nazionale relative alla definizione del processo di gestione degli incidenti di sicurezza informatica, pubblicate a Dicembre 2025.

In data 31 dicembre 2025 l'Agenzia per la Cybersicurezza Nazionale (ACN) ha pubblicato le Linee Guida NIS - Specifiche di base, recanti la definizione del processo di gestione degli incidenti di sicurezza informatica, in attuazione del decreto legislativo 4 settembre 2024, n. 138 (nel seguito il «Decreto NIS») di recepimento della Direttiva (UE) 2022/2555 (NIS2).

In particolare, il documento **descrive in dettaglio il processo di gestione degli incidenti significativi** indicati negli allegati 3 e 4 della determinazione di ACN n. 379907/2025, che i soggetti essenziali e importanti sono obbligati a notificare al CSIRT Italia, come previsto dalla Determinazione di ACN 33017/2025.

Ambito di applicazione e destinatari

Le Linee Guida sono rivolte ai soggetti NIS essenziali e importanti, pubblici e privati, che rientrano nell'ambito di applicazione del Decreto NIS.

Il documento fornisce un modello di riferimento per la definizione di un processo strutturato e coerente di gestione degli incidenti di sicurezza informatica, idoneo a soddisfare gli obblighi previsti dalla normativa.

Il processo di gestione degli incidenti

Il modello di processo delineato dall'ACN è ispirato alle best practice internazionali e, in particolare, al framework NIST Incident Response. Il processo si articola in cinque fasi, articolate nei seguenti paragrafi.

1. Preparazione

La fase di preparazione precede il verificarsi dell'incidente e costituisce il presupposto fondamentale per una gestione efficace degli eventi di sicurezza. Essa comprende le attività di governo, identificazione e protezione.

In tale fase, il soggetto NIS è chiamato a definire politiche di sicurezza informatica, assegnare ruoli e responsabilità, predisporre un piano di gestione degli incidenti e adottare misure tecniche e organizzative di prevenzione.

1.1 Governo: la sotto-fase di governo riguarda la definizione delle politiche di sicurezza informatica, dei ruoli e delle responsabilità e del piano di gestione degli incidenti, e deve essere approvato dagli organi direttivi.

1.2 Identificazione: la sotto-fase di identificazione include l'inventario dei sistemi informativi e di rete e l'individuazione di minacce e vulnerabilità.

1.3 Protezione: la sotto-fase di protezione prevede l'adozione di misure tecnologiche e organizzative volte a prevenire gli incidenti e limitarn l'impatto.

2. Rilevamento

La fase di rilevamento è finalizzata a individuare tempestivamente eventi rilevanti per la sicurezza informatica tramite attività di monitoraggio proattive e reattive, anche mediante strumenti tecnologici avanzati.

3. Risposta

La fase di risposta comprende le attività di segnalazione, investigazione, contenimento ed eradicazione. Particolare rilievo assumono gli obblighi di notifica degli incidenti significativi al CSIRT Italia.

3.1 Segnalazione: la segnalazione riguarda la notifica degli incidenti significativi al CSIRT Italia entro i termini previsti dalla normativa NIS.

3.2 Investigazione: l'investigazione è finalizzata a ricostruire la dinamica dell'incidente e individuarne la causa.

3.3 Contenimento ed eradicazione: il contenimento e l'eradicazione mirano a circoscrivere l'incidente e rimuovere le minacce dai sistemi.

4. Ripristino

Il ripristino è volto a riportare i sistemi informativi e di rete allo stato antecedente all'incidente, assicurando la continuità operativa e il corretto funzionamento dei servizi.

5. Miglioramento continuo

La fase di miglioramento si basa sull'analisi post-incidente e sulle lezioni apprese, con l'obiettivo di rafforzare progressivamente la capacità di gestione degli incidenti.

Gli allegati alle linee guida

Appendice A – Introduzione alle specifiche di base

L'Appendice A introduce la struttura e la logica delle specifiche di base della disciplina NIS.

Appendice B – Misure di sicurezza per la gestione degli incidenti

L'Appendice B elenca le misure di sicurezza di base associate alle diverse fasi del processo di gestione degli incidenti.

Conclusioni

Le Linee Guida ACN configurano la gestione degli incidenti di sicurezza informatica come elemento essenziale della resilienza operativa dei soggetti NIS, trasformando l'adempimento normativo in leva strategica di governance e continuità dei servizi.

Per eventuali ulteriori informazioni e approfondimenti specifici, restiamo a disposizione per un confronto dedicato.

CONTATTI

BDO Law S.r.l. Sta
Viale Abruzzi, 94
20131 Milano
Tel. 02 58 20 10

bdolaw@bdo.it

BDO è tra le principali organizzazioni internazionali di servizi professionali alle imprese.

Audit | Advisory | Digital | Tax | Law

www.bdo.it

NEWSLETTER

Vuoi ricevere le notizie da BDO direttamente via email?
Iscriviti alle nostre mailing list.