I nuovi obblighi di sicurezza IT stabiliti dalla Legge 90/2024

Focus sui soggetti essenziali

Informazioni documento
Versione 4.0
20 agosto 2026

Ing. Francesco Volani
Computer Systems Engineer - MEng - MBCS - CITP® - CISA® - CISM® - CRISC® - CGEIT® - CDPSE® - CSA STAR™ - CPMA - CPSM - ISO/IEC 27001 LA / 20000 LA / 42001 AI MSA - ISO 22301 LA - ISO 19011 - NIST CSF - COBIT® - ITIL®

La Legge 90/2024 ha anticipato, integrato e rafforzato alcuni aspetti del *quadro di cybersicurezza* che è stato completato dal recepimento della Direttiva NIS2 tramite il D.Lgs. 138/2024. In particolare la Legge stabilisce il ruolo di coordinamento operativo[1] e sanzionatorio[2] dell'Agenzia per la Cybersicurezza Nazionale (ACN, l'autorità italiana responsabile della tutela degli interessi nazionali nel campo della sicurezza cibernetica) in relazione ai *soggetti essenziali e importanti* ai sensi del decreto NIS.

Risulta di particolare rilevanza la determinazione del 14 aprile 2025 (n. 164179/2025) successivamente aggiornata il 18 dicembre 2025 (n. 379907/2025) a firma del Direttore Generale dell'Agenzia per la cybersicurezza nazionale[3] che stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi del Decreto Legge 138/2024[4]. Nello specifico, gli articoli 24 e 25 sono declinati nella Determinazione ACN dall'art. 2 (*adozione delle specifiche di base*) e art. 3 (*termini per l'adozione delle specifiche di base*) che **impongono precise e puntuali misure di sicurezza e procedure di gestione degli incidenti** articolati, per i soggetti essenziali, negli allegati 2 e 4 della determina.

Per i soggetti identificati nel 2025, i **termini di adozione**, in ordine cronologico, sono stabiliti nei seguenti:

- procedure di gestione degli incidenti (allegato 4 della determina): **31 dicembre 2025**
- misure di sicurezza (allegato 2 della determina): **30 settembre 2026**

[1] art. 2 e art. 6
[2] art. 11
[3] di cui all'articolo 31, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138
[4] art. 23 - Organi di amministrazione e direttivi; art. 24 - Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica; art. 25 - Obblighi in materia di notifica di incidente; art. 29 - Banca dei dati di registrazione dei nomi di dominio; art. 32 - Previsioni settoriali specifiche

Il recente aggiornamento del 13 aprile 2026 (determinazione 127434/2026) integra la determina 2025 (determinazione 379907/2025) rilanciando gli obblighi per i nuovi soggetti NIS iscritti nel 2026, identificando - solo per tali soggetti - le nuove scadenze.

Le procedure di gestione degli incidenti per i soggetti essenziali

L'allegato 4 alla determinazione ACN riassume gli *incidenti significativi* di base che i soggetti essenziali devono tassativamente essere in grado di gestire entro 9 mesi dalla data di inserimento del soggetto NIS nell'elenco dei soggetti NIS di ACN, ovvero per i soggetti iscritti nel 2025 entro il 31 dicembre 2025. Questi sono definiti sinteticamente nei seguenti:

Codice	**Descrizione**
IS-1	Il soggetto NIS ha evidenza della perdita di *riservatezza*, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di *integrità*, con impatto verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Il soggetto NIS ha evidenza della violazione dei *livelli di servizio attesi* dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01.
IS-4	Il soggetto NIS ha evidenza, anche sulla base dei parametri quali-quantitativi definiti ai sensi della misura DE.CM-01, dell'accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.

Come si evince, la categorizzazione degli incidenti riportata in tabella si riferisce essenzialmente agli attributi di riservatezza, integrità e disponibilità delle informazioni propri dello standard ISO/IEC 27001, con l'indicazione aggiuntiva della capacità, da parte del soggetto NIS, di essere in grado di rilevare e dimostrare eventuali accessi non autorizzati o abusi dei privilegi di accesso ai propri dati digitali, attraverso adeguati strumenti di monitoraggio e registrazione.

E' opportuno ricordare che la definizione di "incidente significativo" è originariamente riportata all'interno della Direttiva NIS2, con specifico riferimento all'art. 23 "Obblighi di segnalazione", ovvero come riporta il comma 3:

> *3. Un incidente è considerato significativo se:*
>
> *a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;*
> *b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.*

Con la Determinazione del Direttore Generale dell'Agenzia per la cybersicurezza nazionale del 9 febbraio 2026 inserita in Gazzetta Ufficiale (serie generale n. 39) relativa alla *tassonomia degli*

incidenti di cui all'articolo 1, comma 1, della legge 90/2024 vengono identificate le classi di incidenti da segnalare e notificare per tutti i soggetti interessati ovvero le classi IS-1, IS-2 e IS-3 di cui al già citato allegato 4 che corrispondono alle classi dell'allegato 3.

E' doveroso notare come la citata determinazione in Gazzetta Ufficiale indichi un'unica tassonomia sia per i soggetti essenziali che per quelli importanti. Infatti la determina recita espressamente che "[...] la tassonomia da individuare ai sensi della legge 28 giugno 2024, n. 90 è coerente con le fattispecie di «incidenti significativi di base» ai sensi dell'allegato 3 alla determinazione citata" e che "[...] in un'ottica di semplificazione degli oneri da parte dei soggetti interessati" si può "[...] considerare assolto, in caso di prenotifica e notifica effettuata ai sensi dell'art. 25 del decreto NIS, anche l'obbligo di cui all'art. 1, comma 1, della legge n. 90 del 2024 [...]". Tale passaggio giustifica pertanto l'uso di un'unica tassonomia per entrambi i soggetti (essenziali e importanti).

Il recente aggiornamento del 13 aprile 2026 (determinazione 127434/2026) integra la determina 2025 (determinazione 379907/2025) rilanciando gli obblighi per i nuovi soggetti NIS iscritti nel 2026, identificando - solo per tali soggetti - le nuove scadenze.

La gestione degli incidenti è pertanto aspetto che deve trovare già alla data attuale (luglio 2026) concreta declinazione regolamentare, organizzativa ed operativa all'interno delle organizzazioni individuate dalla norma. A titolo d'esempio non esaustivo: policy e procedure di gestione degli incidenti, attività di formazione dell'utenza interessata, attività di monitoraggio e rendicontazione, attività di test periodico dei processi di gestione degli incidenti, rendicontazione ai board, integrazione con i processi di analisi e gestione del rischio informatico.

Specifici chiarimenti riguardanti gli *incidenti significativi di base* sono stati formulati da ACN sul proprio portale nella sezione NIS > Domande frequenti > Misure di sicurezza e notifica di incidenti.

Le misure di sicurezza di base per i soggetti essenziali

L'allegato 2 alla determinazione ACN riassume invece le *misure di sicurezza di base* che i soggetti essenziali devono tassativamente attivare entro 18 mesi dalla data di inserimento del soggetto NIS nell'elenco dei soggetti NIS di ACN, ovvero per i soggetti iscritti nel 2025 entro il prossimo 30 settembre 2026.

Le misure possono essere riassunte nelle categorie che seguono. Ogni categoria è declinata in misure specifiche stabilite nell'allegato 2 che riflettono, in ultima istanza, il Cybersecurity Framework del NIST.

Categorie	Sezione

Governo (Govern)	Contesto organizzativo (GV.OC): Il contesto – missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali – che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso
	Strategia di gestione del rischio (GV.RM): Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo
	Ruoli, responsabilità e correlati poteri (GV.RR): Sono stabiliti e comunicati i ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo.
	Politica (GV.PO): La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.
	Gestione del rischio di cybersecurity della catena di approvvigionamento (GV.SC): I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.
Identificazione (Identify)	Gestione degli asset (ID.AM): Gli asset (ad esempio, dati, hardware, software, sistemi, infrastrutture, servizi, persone) che consentono all'organizzazione di raggiungere gli obiettivi di business sono identificati e gestiti in coerenza con la loro importanza rispetto agli obiettivi organizzativi e alla strategia sul rischio dell'organizzazione.
	Valutazione del rischio (Risk Assessment) (ID.RA): È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.
	Miglioramento (ID.IM): I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.
Protezione (Protect)	Gestione delle identità, autenticazione e controllo degli accessi (PR.AA): L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.
	Consapevolezza e formazione (PR.AT): Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity.
	Sicurezza dei dati (PR.DS): I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.
	Sicurezza delle piattaforme (PR.PS): L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.
	Resilienza dell'infrastruttura tecnologica (PR.IR): Le architetture di sicurezza sono gestite in accordo con la strategia sul rischio dell'organizzazione per

	proteggere la riservatezza, l'integrità e la disponibilità degli asset e la resilienza organizzativa.
Rilevamento (Detect)	Monitoraggio continuo (DE.CM): Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.
Risposta (Respond)	Gestione degli incidenti (RS.MA): Le risposte agli incidenti di cybersecurity rilevati sono gestite.
	Segnalazione e comunicazione della risposta agli incidenti (RS.CO): Le attività di risposta sono coordinate con gli stakeholder interni ed esterni come richiesto da leggi, regolamenti o politiche.
Ripristino (Recover)	Esecuzione del piano di ripristino dagli incidenti (RC.RP): Le attività di ripristino sono eseguite per garantire la disponibilità operativa dei sistemi e dei servizi interessati da incidenti di cybersecurity.
	Comunicazione sul ripristino dagli incidenti (RC.CO): Le attività di ripristino sono coordinate con le parti interne ed esterne.

Le macro-categorie riportate rispondono concordemente alle attese della Direttiva NIS2, con particolare riferimento all'art. 21 "Misure di gestione dei rischi di cibersicurezza".

E' opportuno notare come le misure indicate abbiano prima di tutto un impatto nel complessivo *governo della sicurezza*, con successive e conseguenti declinazioni operative derivanti essenzialmente da una gestione continua del rischio finalizzata a identificare le più opportune misure di sicurezza da implementare secondo attività pianificate e controllate.

L'allegato 4 organizza le singole sezioni anche in *ambiti* come di seguito elencato:

Ambito
Affidabilità delle risorse umane
Conformità e audit di sicurezza
Continuità operativa, ripristino in caso di disastro e gestione delle crisi informatiche
Formalizzazione politiche e procedure operative
Formazione del personale e consapevolezza
Gestione degli asset
Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento
Gestione del rischio
Gestione dell'autenticazione, delle identità digitali e del controllo accessi
Gestione delle vulnerabilità
Monitoraggio degli eventi di sicurezza

Protezione delle reti e delle comunicazioni
Risposta agli incidenti e ripristino
Ruoli e responsabilità
Sicurezza dei dati
Sicurezza fisica
Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete

L'implementazione delle misure di sicurezza di base è aspetto che dovrà trovare piena attuazione alla scadenza del prossimo 30 settembre 2026, con opportuna declinazione regolamentare, organizzativa ed operativa all'interno delle organizzazioni individuate dalla norma. A titolo d'esempio non esaustivo: politiche e procedure di sicurezza delle informazioni; sistemi di analisi e gestione del rischio informatico; ruoli e organizzazione della sicurezza IT; piano programmatico per la sicurezza di dati, sistemi e infrastrutture; interventi di potenziamento delle capacità per la gestione dei rischi informatici; pianificazione e attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate da ACN; monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

Specifici chiarimenti riguardanti le *misure di sicurezza di base* sono stati formulati da ACN sul proprio portale nella sezione NIS > Domande frequenti > Misure di sicurezza e notifica di incidenti.

La determinazione del 22 luglio 2025 (determinazione 283727/2025) successivamente aggiornata il 19 settembre 2025 (determinazione 250916/2025) a firma del Direttore Generale dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 7, comma 6 del DL 138/2024 stabilisce inoltre le procedure attuative in riferimento al Decreto NIS definendo rigorosamente i termini e le modalità per l'utilizzo e l'accesso alla piattaforma digitale NIS, uno strumento essenziale attraverso cui i soggetti NIS devono comunicare con l'Autorità nazionale competente. Vengono specificate le procedure per il censimento degli utenti e la designazione di figure chiave, come il *Punto di Contatto* e il *Referente CSIRT*, i quali sono responsabili dell'interlocuzione con l'ACN.

La Determina sottolinea che la vigilanza su tali adempimenti e la responsabilità per eventuali violazioni ricadono sugli organi di amministrazione e direttivi dei soggetti NIS.

In data 11 agosto 2026 ACN ha infine pubblicato le FAQ relative alle attività di monitoraggio, vigilanza ed esecuzione che svolge quale Autorità nazionale competente NIS con l'obiettivo di contribuire a chiarire gli ambiti, i principi e le modalità di esercizio nei confronti dei soggetti NIS.