DECRETO NIS 2: SOGGETTI INTERESSATI E ADEMPIMENTI PREVISTI

Il D.Lgs. 4 settembre 2024 n. 138, cd. Decreto NIS 2, entrato in vigore il 16.10.2024, ha recepito la Direttiva UE n. 2022/2555 relativa alle misure per un livello comune elevato di cybersicurezza nell'Unione Europea.
Il D.Lgs. n. 138/2024 ha introdotto una nuova disciplina che mira ad assicurare un elevato livello di sicurezza informatica nei soggetti pubblici e privati come specificatamente individuati dalla norma.
Il Decreto NIS 2, oltre a prevedere la Strategia nazionale di cybersicurezza e la disciplina della gestione di crisi informatiche, affida all'Agenzia per la cybersicurezza nazionale (ACN) il compito di vigilare sull'implementazione e sull'attuazione degli adempimenti previsti, nonché al Computer Security Incident Response Team dell'ACN (CSIRT Italia) la funzione di Autorità competente per gli incidenti di sicurezza informatica.
A seguito del Decreto NIS 2, l'ACN è intervenuta con alcuni provvedimenti per fornire i necessari chiarimenti. Si tratta in particolare di:
-Determinazione ACN 379887/2025, pubblicata il 18.12.2025 in sostituzione della Determinazione ACN n. 333017/2025, che definisce l'ambito di applicazione della normativa, le modalità di designazione del punto di contatto e del sostituto, il procedimento per la registrazione e l'aggiornamento delle informazioni di cui all'articolo 7 del Decreto NIS;
- Linee Guida che forniscono indicazioni per la comprensione e l'interpretazione delle specifiche di base, nonché suggeriscono un modello per il processo di gestione degli incidenti e descrivono la relazione tra le fasi del processo e le misure di sicurezza di base;
- Determinazione ACN n. 379907/2025, pubblicata il 23.12.2025, che dà atto del perfezionamento della procedura di informazione delle regole tecniche (cd. notifica TRIS), disciplina le previsioni transitorie inerenti all'obbligo di notifica per gli operatori di servizi essenziali e operatori telco, nonché apporta affinamenti agli obblighi di base.

Di seguito ci si soffermerà su alcuni aspetti ritenuti di maggior rilievo al fine di fornire un quadro della disciplina.

1. I soggetti interessati

L'art. 3 del Decreto NIS 2 individua l'ambito applicativo della normativa comunitaria.
Il Decreto NIS 2 si applica alle Pubbliche Amministrazioni individuate nell'Allegato III. Si tratta di amministrazioni centrali, amministrazioni regionali, amministrazioni locali aventi determinati requisiti dimensionali, altri soggetti pubblici.
La disciplina si applica altresì ai soggetti imprese che operano in determinati ambiti rientranti nelle categorie individuate dagli Allegati I e II e che superano i limiti dimensionali delle piccole imprese (imprese con più di 50 dipendenti ed un fatturato o bilancio annuo superiore ai 10 milioni di euro).
L'Allegato I si riferisce alle sole imprese che operano in settori cd. ad alta criticità, mentre l'Allegato II si riferisce alle imprese che operano in altri settori critici.
Ai sensi dell'art. 6 del Decreto NIS 2, tali imprese si distinguono in:
- soggetti essenziali, definiti al comma 1;
- soggetti importanti.
In ragione della tipologia di soggetto (essenziale o importante), l'ACN ha declinato gli obblighi relativi alle misure di sicurezza di base e di gestione degli incidenti che le imprese devono adottare.
A prescindere dai limiti dimensionali, il Decreto NIS 2 si applica ad ulteriori soggetti individuati all'art. 3 co. 5, ai soggetti rientranti nell'Allegato IV, nonché ai soggetti individuati ai commi 9 e 10 del medesimo art. 3.

2. Gli adempimenti previsti per l'adeguamento al Decreto NIS 2

2.1. Aggiornamento annuale

La normativa (art. 7 Decreto NIS 2) prevede un aggiornamento annuale da farsi tra il 1 gennaio ed il 28 febbraio.
Tale obbligo riguarda i soggetti NIS già registratisi in piattaforma nel 2025, i quali devono aggiornare la propria registrazione e presentare una nuova dichiarazione, tramite il Portale dei Servizi ACN, confermando o modificando i dati della precedente dichiarazione.
Nel medesimo periodo, i soggetti non registrati sono chiamati a valutare la propria posizione e registrarsi sul Portale ACN nel caso in cui ritengano che la normativa sia a loro applicabile.
Le modalità di registrazione e aggiornamento sono meglio precisate nella Determinazione ACN n. 379887/2025 del 18.12.2025.
L'art. 7 richiede inoltre di procedere a comunicare o aggiornare altre informazioni tra il 15 aprile e 31 maggio di ogni anno.

Preme evidenziare che la mancata registrazione, comunicazione o aggiornamento delle informazioni richieste ai sensi dell'art 7 del Decreto NIS 2 sono punite ai sensi dell'art. 38 del medesimo Decreto.

2.2. Obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente

Da gennaio 2026 e comunque entro i 9 mesi successivi alla notifica di inserimento nell'elenco dei soggetti NIS, vige per i soggetti NIS l'adempimento dell'obbligo di notifica degli incidenti significativi di base previsti all'art. 25 del D.Lgs. 138/2024 e descritti negli Allegati 3 e 4 alla Determinazione ACN n. 379907/2025 a cui si rinvia.

Le "Linee Guida NIS – Definizione del processo di gestione degli incidenti di sicurezza informatica" definiscono la gestione degli incidenti come "*l'insieme delle attività volte a rilevare tempestivamente un incidente, a rispondervi in modo appropriato ed efficiente, a ripristinare la situazione allo stato antecedente al verificarsi dello stesso e a migliorare la capacità di rispondere a futuri incidenti tramite le lezioni apprese"* e ritengono che tale gestione rappresenti *"una capacità essenziale per garantire la continuità delle attività e dei servizi, la protezione delle informazioni e la resilienza delle organizzazioni*".

Il processo di gestione degli incidenti viene suddiviso nelle seguenti fasi.

a) Preparazione: riguarda "*le attività propedeutiche volte a garantire una gestione strutturata ed efficace degli incidenti di sicurezza*" ed include le attività di governo, identificazione e protezione.
   Tra tali attività rientrano:
   - la predisposizioni di una politica di sicurezza informatica anche in materia di sicurezza per la gestione degli incidenti;
   - l'individuazione dei ruoli e delle responsabilità per le varie fasi del processo di gestione degli incidenti (tra cui la nomina del Referente CSIRT da parte del Punto di Contatto);
   - l'inventario dei sistemi informativi e di rete e l'individuazione di minacce e vulnerabilità;
   - l'individuazione delle misure di protezione tecnologiche ed organizzative volte a ridurre la probabilità di accadimento e limitare l'impatto degli incidenti.
b) Rilevamento: ha lo scopo di "*individuare e analizzare gli eventi rilevanti per la sicurezza informatica con l'obiettivo di individuare tempestivamente il verificarsi di un incidente e limitarne l'impatto e l'estensione*".
c) Risposta: inizia nel momento in cui è stato dichiarato l'incidente e rappresenta la fase centrale del processo di gestione degli incidenti. Tale fase include le attività di investigazione, notifica, contenimento ed eradicazione dell'incidente.
   "*Sulla base di quanto previsto dal decreto NIS e dalla determinazione obblighi di base, i soggetti NIS sono tenuti a notificare le seguenti tipologie di incidente:*
   • 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.
   I soggetti essenziali devono inoltre notificare la seguente tipologia di incidente:
   • 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."
   In tale fase il soggetto NIS deve avere evidenza dell'incidente occorso in quanto deve disporre di elementi oggettivi dai quali evincere che si è verificato l'incidente di sicurezza informatica. Acquisita l'evidenza dell'incidente, il soggetto NIS deve procedere a segnalare all'autorità competente (CSIRT) la trasmissione della pre-notifica (entro 24 ore) e della notifica (entro 72 ore). Il soggetto NIS deve procedere a segnalare tempestivamente anche alle parti interessate la notifica di incidente. Successivamente al verificarsi dell'incidente il soggetto NIS sarà tenuto a inviare all'autorità competente un'eventuale relazione intermedia ed una relazione finale.
   Viene inoltre esaminato l'incidente in modo approfondito, così da ricostruire il più possibile l'intera sequenza degli eventi occorsi, individuare la causa dell'incidente e valutare l'estensione della compromissione.
   Successivamente è necessario procedere con la sottofase del "*contenimento*", al fine di circoscrivere il perimetro dell'attacco in modo da limitare l'impatto dell'incidente. Di conseguenza, sarà possibile procedere alle attività di "*eradicazione*", rimuovendo "*ogni capacità di controllo e persistenza nella rete da parte dell'attaccante*".
d) Ripristino: ha lo scopo di riportare i sistemi informativi allo stato precedente all'incidente così ripristinando il regolare funzionamento.

e) Miglioramento: deve essere svolto durante tutte le fasi del processo di gestione degli incidenti, in particolare durante l'analisi post incidente al fine di valutare carenze, criticità e l'efficacia della risposta predisposta.

Al fine di gestire gli incidenti, i soggetti NIS sono tenuti a predisporre, sottoporre ad approvazione degli organi di amministrazione e aggiornare periodicamente un piano di continuità operativa, un piano di ripristino in caso di disastro ed un piano di gestione delle crisi.

2.3. Obblighi di adozione delle misure di sicurezza di base

Entro i 18 mesi successivi alla notifica di inserimento nell'elenco dei soggetti NIS, i soggetti NIS devono adottare le misure di sicurezza di base previste dall'art. 24 del Decreto NIS 2.

Le misure di sicurezza devono essere applicate ai sistemi informativi e di rete dei soggetti NIS. Le misure di sicurezza devono essere adeguate ai rischi esistenti, proporzionate al grado di esposizione e alle dimensioni di ciascun soggetto, nonché alla probabilità di verifica di incidenti e alla loro gravità.

Le misure di sicurezza da adottare devono altresì rispettare requisiti organizzativi e tecnologici, nonché devono fondarsi su documenti di cui il soggetto è in possesso o che devono essere elaborati *ad hoc* (tra cui inventari, elenchi, piani, politiche di sicurezza informatica, registri, procedure).

In particolare, le misure di sicurezza da adottare devono comprendere almeno i seguenti elementi:

- politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
- gestione degli incidenti (tra cui procedure e strumenti);
- continuità operativa (tra cui gestione back up, ripristino in caso di disastro e gestione delle crisi);
- sicurezza della catena di approvvigionamento;
- sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete:
- politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;
- pratiche di igiene di base e di formazione;
- politiche e procedure relative all'uso della crittografia;
- sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;
- uso di soluzioni di autenticazione a più fattori.

Ciascun soggetto deve quindi predisporre le misure di sicurezza di base previste dagli Allegati 1 e 2 della Determinazione ACN n. 379907/2025 a cui si rinvia.

3. Punto di contatto, sostituto punto di contatto e Referente CSIRT

Il Punto di contatto, ai sensi della Determinazione ACN n. 379887/2025 del 18.12.2025, è "*una persona fisica designata dal soggetto NIS con il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso*".

Il Punto di contatto è supportato nell'esercizio delle proprie funzioni dal Sostituto punto di contatto, il quale può interloquire direttamente con l'ACN ed effettuare le medesime azioni del punto di contatto ad eccezione della registrazione di cui all'art. 7 Decreto NIS.

Il Punto di contatto deve, a sua volta, designare il Referente CSIRT, il quale ha il compito di interloquire con CSIRT Italia ed effettuare le necessarie notifiche di incidente.

4. Responsabilità degli Organi di amministrazione e direttivi

Ai sensi dell'art. 23 del D.Lgs. 138/2024, gli organi di amministrazione e direttivi dei soggetti NIS devono approvare le modalità di implementazione delle misure di gestione dei rischi e sovrintendere all'implementazione degli obblighi previsti. Essi, inoltre, sono responsabili delle violazioni in materia NIS 2 e sono tenuti a eseguire una formazione specifica in materia, nonché provvedere ad una formazione coerente e periodica per i propri dipendenti.

5. Sanzioni

Il Capo V del Decreto NIS 2 disciplina le attività di monitoraggio, vigilanza ed esecuzione, nonché le conseguenti sanzioni che l'ACN può emettere nei confronti dei soggetti NIS.

Ai sensi dell'art. 38, co. 4 del Decreto NIS 2, laddove il soggetto NIS non adempia nei termini stabiliti dalla normativa, l'ACN può sospendere temporaneamente in parte o per intero i servizi o le attività pertinenti svolti dal soggetto inadempiente.

Inoltre, al rappresentante legale o ai soggetti dirigenziali, in caso di inadempimento, è possibile applicare la sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto.

A tali sanzioni, infine, si affiancano le sanzioni amministrative pecuniarie previste dai commi 8 e seguenti dell'art. 38.