CIRCOLARE 25/2025
30/10/2025

RELEVANT
BUSINESS MATTERS

I NUOVI OBBLIGHI IN MATERIA DI SICUREZZA INFORMATICA – AGGIORNAMENTI OPERATIVI

A CURA DI

LUIGI MELLONI
CHIARA CERVELLIN

Premessa

Con la presente desideriamo dare seguito alla nostra precedente Circolare n. 8/2025 del 19 febbraio 2025, relativa ai **nuovi obblighi in materia di sicurezza informatica** imposti dalla normativa in materia di Cybersicurezza nell'Unione Europea recata dal D. Lgs. 4 settembre 2024, n. 138, cd. "***Decreto Nis***", di recepimento della Direttiva (UE) 2022/2555 (o "*NIS 2*").
Come precedentemente comunicato, l'obbligo di registrazione sulla piattaforma digitale dell'Agenzia per la Cybersicurezza Nazionale (ACN) è spirato il 28 febbraio 2025[1]. Tuttavia, a partire dal 14 aprile 2025, è stato riattivato sul portale dell'ACN il servizio per la registrazione tardiva.

Si ricorda, in via di estrema sintesi, che il Decreto NIS individua i soggetti obbligati, sia pubblici che privati, sulla base di specifici requisiti settoriali e dimensionali. Tali soggetti sono distinti in due categorie di "essenziali" e "importanti", cui corrispondono obblighi di sicurezza modulati in base alla classificazione.
Lo schema seguente, elaborato dall'ACN, riassume visivamente i settori merceologici interessati e i requisiti dimensionali[2] richiesti:

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia	19 tipologie di soggetto	Essenziali	Importanti *	Fuori ambito **
Trasporti	10 tipologie di soggetto			
Settore bancario	DORA Lex specialis			
Infrastrutture dei mercati finanziari				
Settore sanitario	5 tipologie di soggetto			
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto		Importanti *	Fuori ambito **
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto	Importanti *		Fuori ambito **
Gestione dei rifiuti	1 tipologia di soggetto			
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto			
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto			
Fabbricazione	6 tipologie di soggetto			
Fornitori di servizi digitali	4 tipologie di soggetto			
Ricerca	2 tipologie di soggetto	Importanti *		Fuori ambito **
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale	4 categorie di PA	Essenziali		
Pubblica Amministrazione regionale e locale	11 categorie di PA	Importanti *		
Ulteriori tipologie di soggetti	4 tipologie di soggetti	Identificazione dell'Autorità		

Schema degli ambiti di applicazione
* Possibile identificazione dell'Autorità come essenziali
** Possibile identificazione dell'Autorità come importanti o essenziali

[1] Per talune categorie di fornitori di servizi digitali, elencati all'art. 1, comma 3, lett. a), del D.Lgs. n. 138/2024, il termine per la registrazione era fissato al 17 gennaio 2024.
[2] Le grandi imprese sono quelle che occupano almeno 250 dipendenti oppure presentano un fatturato annuo di almeno a 50 milioni di euro o un totale di bilancio di almeno 43 milioni di euro. Le medie imprese sono invece quelle che occupano almeno 50 dipendenti oppure hanno un fatturato annuo di almeno 10 milioni di euro o un totale di bilancio di almeno 10 milioni di euro.

Per l'individuazione puntuale di tutti i settori, sottosettori e delle specifiche tipologie di soggetto tenute agli adempimenti, è indispensabile fare riferimento alla documentazione ufficiale disponibile sul portale dell'Agenzia per la Cybersicurezza Nazionale al seguente link: https://www.acn.gov.it/portale/nis/ambito, nonché alle FAQ disponibili sul sito dell'ACN.

Successivamente alla registrazione sulla piattaforma dell'Agenzia per la Cybersicurezza Nazionale (ACN), **le organizzazioni dovrebbero avere ricevuto la comunicazione di inserimento nell'elenco nazionale dei soggetti NIS** predisposto dall'ACN, e sono ora chiamate ad affrontare le fasi successive del percorso di adeguamento alla nuova normativa[3].

Alla data odierna, le principali scadenze operative sono le seguenti:

- dal 20.11.2025 al 31.12.2025 - nomina del referente CSIRT;
- gennaio 2026 (indicativamente) – obblighi di notifica degli incidenti significativi;
- dall'1.1.2026 al 28.2.2026 e dal 15.4.2026 al 31.5.2026 - aggiornamento informazioni;
- ottobre 2026 (indicativamente) - adozione delle misure di sicurezza di base.

Di seguito si fornisce un breve commento per ciascuna delle scadenze sopra indicate.

NOMINA DEL REFERENTE CSIRT- a partire dal 20 novembre p.v. ed entro il 31 dicembre p.v.

A partire dal 20 novembre p.v. ed entro il 31 dicembre 2025, il Punto di Contatto[4] di ciascuna organizzazione dovrà procedere alla nomina del Referente CSIRT, una persona fisica designata per interfacciarsi direttamente con lo CSIRT Italia.
La sua nomina dovrà essere effettuata tramite la procedura telematica dedicata, resa disponibile sul portale dell'ACN. Nell'ambito della stessa procedura, sarà possibile indicare uno o più sostituti, al fine di garantire continuità operativa e tempestività nelle comunicazioni.
Il referente – così come gli eventuali sostituti – dovrà essere in possesso di competenze tecniche informatiche e sarà responsabile della notifica tempestiva degli incidenti.
Si veda, a tale proposito, la Determinazione dell'ACN del 19 settembre 2025 al seguente link: https://www.acn.gov.it/portale/documents/d/guest/detacn_piattaformanis_250916-v5_signed

NOTIFICA DEGLI INCIDENTI SIGNIFICATIVI - a partire da 9 mesi dalla notifica di inserimento nell'elenco dei soggetti NIS

I soggetti rientranti nell'ambito di applicazione del decreto NIS, sono tenuti a notificare al CSIRT Italia

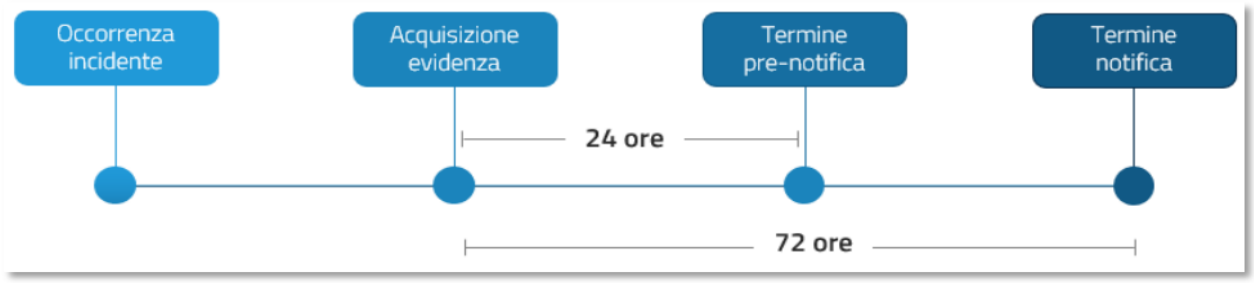
[3] Ai fini dell'individuazione dei soggetti tenuti all'obbligo di registrazione e dei settori interessati dalla disciplina in esame, si rinvia a quanto già comunicato con la nostra precedente Circolare n. 8 e si invita a verificare gli ulteriori dettagli direttamente sul sito dell'ACN.
[4] In estrema sintesi, il Punto di Contatto è la figura individuata nel rappresentante legale, in un procuratore generale oppure in un dipendente del soggetto rientrante nel perimetro del Decreto NIS, con la funzione di fungere da interlocutore ufficiale tra l'organizzazione e l'ACN. È inoltre responsabile dell'accesso e dell'utilizzo della piattaforma digitale dell'ACN per la registrazione del soggetto e per l'invio di comunicazioni obbligatorie previste dalla normativa in esame.

(*Computer Security Incident Response Team*) gli incidenti significativi di base[5] che hanno un impatto sulla fornitura dei loro servizi e che sono indicati negli **allegati 3 e 4 della Determinazione dell'ACN 164179 del 14 aprile 2025**. L'art. 3, comma 2, della Determinazione appena citata stabilisce inoltre che "*il termine per l'adempimento dell'obbligo di notifica degli incidenti significativi di base descritti negli allegati 3 e 4* ***è fissato in nove mesi dalla ricezione, da parte del soggetto NIS, della comunicazione di inserimento nell'elenco dei soggetti NIS***".
Ciascuna tipologia di incidente significativo è costituita da un codice identificativo e da una descrizione. Nel complesso, sono state definite 3 tipologie di incidenti significativi per i soggetti "importanti" e 4 tipologie di incidenti significativi per i soggetti "essenziali".
Nella seguente tabella sono riportati gli incidenti significativi di base previsti dalla Determinazione del 14 aprile 2025: il cerchio di colore blu, nella colona **S_I**, indica che il corrispondente incidente si applica ai soggetti "importanti", mentre il cerchio di colore verde nella colona **S_E** indica che il corrispondente incidente si applica ai soggetti essenziali[6].

CODICE	DESCRIZIONE	S_I	S_E
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 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.		●

Ai fini dell'adempimento dell'obbligo di notifica degli incidenti significativi, rileva il momento in cui il soggetto NIS viene effettivamente a conoscenza del verificarsi di una delle tipologie di incidente previste, ossia quando dispone di elementi oggettivi dai quali si evince il verificarsi dell'incidente di sicurezza informatica. L'acquisizione dell'evidenza è tipicamente successiva al verificarsi dell'incidente e definisce il momento dal quale decorre il termine per la trasmissione della pre-notifica **(24 ore)** e della notifica **(72 ore)** al CSIRT Italia[7].

[5] La dicitura "di base" è utilizzata per indicare il fatto che si tratta di incidenti significativi che i soggetti NIS notificano in fase di prima applicazione del decreto NIS.
[6] Si precisa che la misura "DE.CM-01", indicata nella tabella, si riferisce alle misure di sicurezza di base relative alle reti e ai servizi di rete che i soggetti essenziali ed importanti sono tenuti ad adottare. Per una descrizione dettagliata del contenuto di tali misure, si rinvia al seguente link https://www.acn.gov.it/portale/nis/modalita-specifiche-base ove sono reperibili tutte le misure di sicurezza di base rischieste, ivi compresa quella recante il codice DE.CM-01. Tabella estrapolata dalle Linee Guida NIS.
[7] In sintesi, la pre-notifica dovrebbe, ove possibile, indicare se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero, la notifica dovrebbe aggiornare le informazioni già trasmesse e indicare una valutazione dell'incidente,



[8]

Si rinvia, per ulteriori dettagli, alle già citate linee guida NIS, pubblicate nel mese di settembre 2025, reperibili al seguente indirizzo: https://www.acn.gov.it/portale/documents/d/guest/guida-alla-lettura-specifiche-di-base-2.

AGGIORNAMENTO ANNUALE

Dal 1° gennaio al 28 febbraio di ogni anno, i soggetti NIS sono tenuti registrarsi o aggiornare la propria registrazione sulla piattaforma dell'ACN, tramite il **Servizio NIS/Registrazione**, assicurandosi che le informazioni fornite siano corrette e aggiornate (tra cui, i valori del fatturato e del bilancio, il numero di dipendenti, ecc.).

Dal 15 aprile al 31 maggio di ogni anno, i soggetti NIS sono tenuti ad aggiornare, tramite il **Servizio NIS/Aggiornamento annuale**, le informazioni richieste (tra cui i dati anagrafici e di contatto del soggetto NIS, i dati anagrafici del Punto di Contatto, lo spazio di indirizzamento IP pubblico ecc.), assicurandone la correttezza.

I dettagli relativi al processo di aggiornamento annuale sono disciplinati agli artt. 11 e art. 16 della Determinazione dell'ACN del 19 settembre 2025, reperibile al seguente link: https://www.acn.gov.it/portale/documents/d/guest/detacn_piattaformanis_250916-v5_signed.

Si raccomanda in ogni caso di consultare periodicamente il sito dell'ACN per verificare eventuali aggiornamenti o chiarimenti relativi alle modalità di aggiornamento sopra descritte.

ADOZIONE DELLE MISURE DI SICUREZZA DI BASE - entro 18 mesi dalla notifica di inserimento nell'elenco dei soggetti NIS

I soggetti rientranti nell'ambito di applicazione del Decreto NIS, dispongono di **18 mesi di tempo** dalla ricezione della comunicazione di inserimento nell'elenco dei soggetti NIS **per adottare le misure di sicurezza di base[9], riportate negli allegati 1 e 2 della Determinazione dell'ACN 164179 del 14 aprile 2025**.

Le misure di sicurezza si applicano ai sistemi informativi e di rete che i soggetti utilizzano nelle loro

comprensiva della sua gravità e del suo impatto nonché, ove disponibili, gli indicatori di compromissione. Sono inoltre previste ulteriori incombenze tra cui una relazione finale entro un mese dalla trasmissione della notifica dell'incidente. Si rinvia, per una disamina complete degli obblighi, all' art. 25 D.lgs. 138/2024.

[8] Tabella estratta dalle linee guida NIS.

[9] La dicitura "di base" è utilizzata per indicare il fatto che si tratta delle misure di sicurezza che i soggetti adottano in fase di prima applicazione del Decreto NIS.

attività o nella fornitura dei loro servizi.
Tali misure, differenziate per soggetti "essenziali" (43 misure) e "importanti" (37 misure)[10], sono caratterizzate da un codice identificativo, una descrizione e da uno o più requisiti. In particolare, i requisiti specificano ciò che è richiesto ai fini dell'implementazione delle misure di sicurezza.

Per meglio chiarire la natura di tali adempimenti, si riporta di seguito un esempio di misura di sicurezza di base comune ai soggetti essenziali ed importanti.

Formazione del Personale (Misura PR.AT-01)

Questa misura, tratta dagli Allegati alla citata Determinazione dell'ACN del 14 aprile u.s., mira a garantire che il personale dell'organizzazione possieda le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di *cybersecurity*.
In termini pratici, l'organizzazione deve:

- definire, attuare, aggiornare e documentare un piano di formazione in materia di sicurezza informatica del personale che includa la pianificazione delle attività e i contenuti della formazione fornita e le eventuali modalità di verifica dell'acquisizione dei contenuti. Il piano deve includere anche gli organi di amministrazione e direttivi;
- ottenere l'approvazione formale del piano da parte degli organi di amministrazione e direttivi stessi;
- mantenere un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione, i contenuti trattati e l'esito delle eventuali verifiche di apprendimento.

Per il dettaglio completo di tutte le misure di sicurezza di base e dei relativi requisiti, si rinvia alla documentazione ufficiale pubblicata dall'Agenzia per la Cybersicurezza Nazionale, consultabile al seguente link: https://www.acn.gov.it/portale/nis/modalita-specifiche-base, nonché alle linee guida NIS, pubblicate nel mese di settembre 2025, reperibili al seguente indirizzo: https://www.acn.gov.it/portale/documents/d/guest/guida-alla-lettura-specifiche-di-base-2.

È consigliabile consultare la sezione ufficiale ACN – Servizi NIS o le FAQ aggiornate per verificare eventuali modifiche sopravvenute rispetto al momento di stesura della presente Circolare.

Lo Studio rimane a Vostra completa disposizione per supportarvi nell'interpretazione della normativa.

[10] La distinzione tra soggetti essenziali e importanti è legata alle dimensioni e al settore di appartenenza ed è stata oggetto di approfondimento nella precedente Circolare n. 8/2025, a cui si fa rinvio.

CONTATTI

LUIGI MELLONI

LUIGI.MELLONI@RLVT.IT

CHIARA CERVELLIN

CHIARA.CERVELLIN@RLVT.IT

RLVT
RELEVANT
BUSINESS MATTERS

RLVT – SOCIETÀ TRA PROFESSIONISTI A R.L.
VIA AVOGADRO, 12/A – 10121 TORINO – ITALIA T. +39 011 55 67 222 – INFO@RLVT.IT