



Attuazione del decreto NIS

I prossimi passi

Estensione ambiti di applicazione

- **18 settori: 11 settori altamente critici e 7 settori critici** (originariamente 0)
- **Intera infrastruttura ICT** (originariamente solo reti e sistemi serventi i servizi essenziali)
- Salvo eccezioni, dalle medie imprese in su

Processo di identificazione dei soggetti

- **Identificazione automatica** sulla base di criteri oggettivi
- L'Autorità ha anche la facoltà di identificare ulteriori soggetti

Obblighi e Supervisione

- Misure di sicurezza specifiche e **proporzionate rispetto al rischio**
- Processo di notifica più dettagliato
- Poteri di esecuzione, ispettivi e sanzionatori rafforzati (**allineamento alle sanzioni GDPR**)

D.Lgs. 138/2024 in vigore dal 16 ottobre 2024

Decreto Legislativo NIS (ambito di applicazione)



Ambito di applicazione (articoli 3 e 6, allegati I-IV)

¹ Possibile identificazione dell'Autorità come essenziali

² Possibile identificazione dell'Autorità come importanti o essenziali

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia (+)	19 tipologie di soggetto	Essenziali	Importanti¹	Fuori ambito²
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			
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto			
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			
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale				
Pubblica Amministrazione regionale e locale	11 categorie di PA			
Ulteriori tipologie di soggetti	5 tipologie e 2 criteri aggiuntivi	Identificazione dell'Autorità		

Settori, sottosettori e tipologie di soggetti introdotti dalla NIS2



Decreto Legislativo NIS (Supervisione)

Sanzioni amministrative (articolo 38)

Violazioni gravi

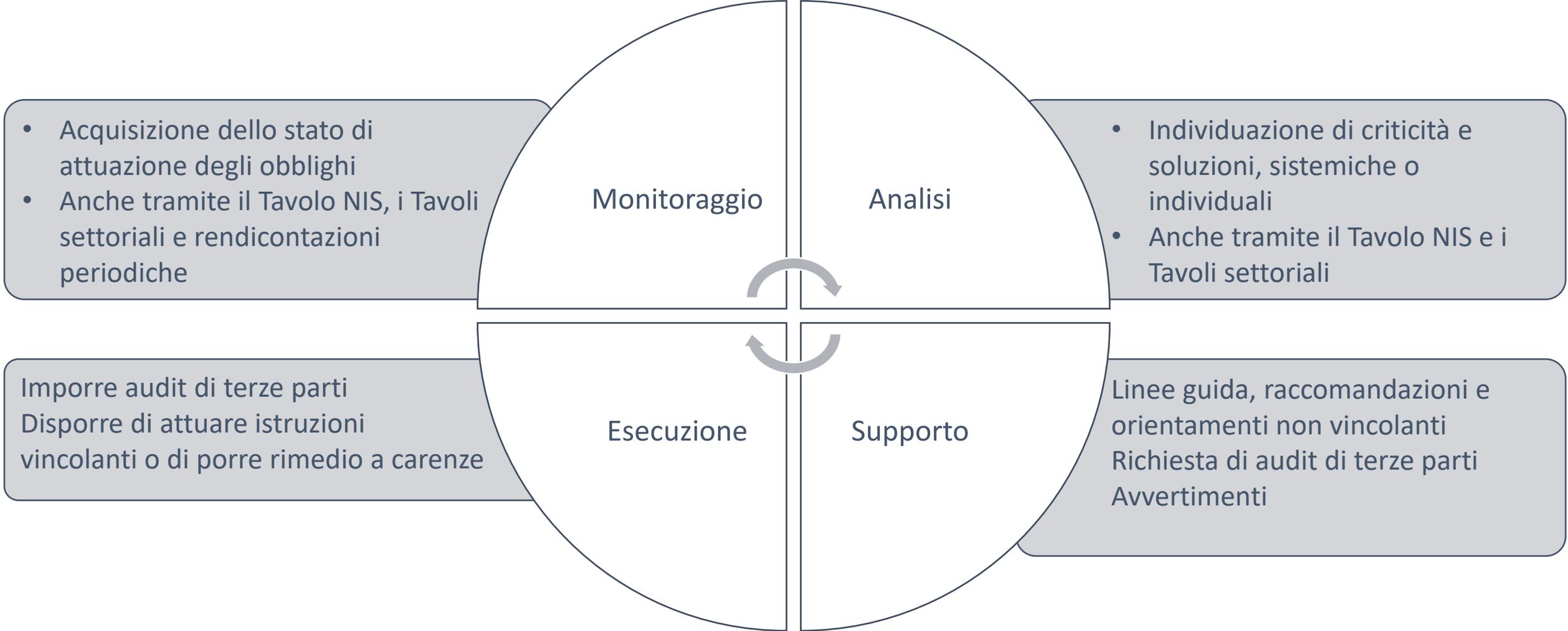
- Mancata osservanza degli obblighi relativi agli organi di amministrazione, alle misure di sicurezza e alle notifiche di incidente
- Inottemperanza alle disposizioni dell'Autorità nazionale competente NIS
- Sanzioni pecuniarie fino a 10 MEUR o 2% per soggetti essenziali e fino a 7 MEUR o 1,4% per soggetti importanti

Altre violazioni

- Mancata registrazione, comunicazione dei dati, osservanza degli obblighi relativi agli obblighi relativi alle certificazioni, alla registrazione dei nomi di dominio e alle previsioni settoriali specifiche
- Sanzioni pecuniarie fino a 0,1% per soggetti essenziali e fino a 0,07% per soggetti importanti

Strumenti deflattivi del contenzioso

Monitoraggio, analisi e supporto (articolo 35) + Poteri di esecuzione (articolo 37)



Decreto Legislativo NIS (Vertici aziendali)



Organi di amministrazione e direttivi: responsabilità e obblighi

Gli organi di amministrazione e direttivi

Approvano le modalità di implementazione delle misure di sicurezza

Sovrintendono all'implementazione degli obblighi

Sono responsabili delle eventuali violazioni



Sono tenuti a seguire una formazione in materia di cybersicurezza

Promuovono la formazione dei propri dipendenti

Decreto Legislativo NIS (Misure di sicurezza)



I dieci ambiti di applicazione delle misure di sicurezza

Politiche di analisi dei rischi e di sicurezza dei sistemi informativi

Gestione degli incidenti

Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi

Sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza dei rapporti con i diretti fornitori o i fornitori di servizi

Sicurezza dell'acquisizione, dello sviluppo e della manutenzione [...], compresa la gestione e la divulgazione delle vulnerabilità

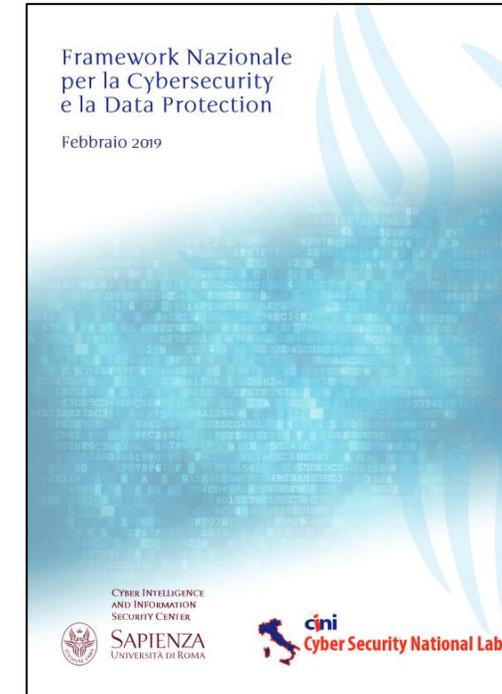
Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza

Pratiche di igiene informatica di base e formazione in materia di cybersicurezza

Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli assetti

Uso di soluzioni di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti



Approccio basato sul rischio e proporzionalità



Le misure di sicurezza si applicano a tutti i sistemi informativi e di rete.



Le misure sono definite secondo un approccio basato sul rischio.



I requisiti sono graduati e adattati sulla base dei rischi effettivi.



Usata la dicitura "*... in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, è ...*".



Le modalità di attuazione del requisito, possono essere adattate al contesto risultante dalla valutazione del rischio.



Linee guida non vincolanti e materiale di supporto

41 misure di sicurezza

- 31 per soggetti essenziali e importanti.
- 10 addizionali solo per i soggetti essenziali.

Struttura misura: codice + descrizione + requisiti

- Il codice identificativo e la descrizione della misura fanno riferimento al FNSC.
- I requisiti indicano ciò che è richiesto ai fini dell'implementazione.

120 requisiti

- 72 per soggetti essenziali e importanti.
- 48 addizionali solo per i soggetti essenziali.

Struttura misure di sicurezza e proporzionalità

ID.RA-05 ← Codice identificativo

Minacce, vulnerabilità, probabilità e impatti sono utilizzati per comprendere il rischio inerente e per informare la prioritizzazione della risposta al rischio. ← Descrizione misura

Specifiche
requisiti

PUNTO	REQUISITO	S_I	S_E
1	In accordo al processo di gestione del rischio di cybersecurity di cui alla misura GV.RM-03, è eseguita e documentata la valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete, comprendendo almeno: <ul style="list-style-type: none"> a) l'identificazione del rischio; b) l'analisi del rischio; c) la ponderazione del rischio. 	●	●
2	La valutazione del rischio di cui al punto 1 è eseguita a intervalli pianificati e almeno con cadenza annuale, nonché qualora si verificano incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi.	●	●
3	La valutazione del rischio di cui al punto 1 è effettuata considerando le minacce interne ed esterne, le vulnerabilità, le probabilità di accadimento e i conseguenti impatti, nonché le eventuali dipendenze da fornitori e partner terzi.		●

Decreto Legislativo NIS (Notifica di incidente)





L'OBBLIGO DI NOTIFICA DECORRE A PARTIRE DAL 1 GENNAIO 2026



NOTIFICHE VOLONTARIE POSSIBILI FIN DA SUBITO



Tassonomia incidenti

BOZZA

IS-1

Il soggetto ha evidenza dell'accesso non autorizzato o abusivo ai dati digitali di proprietà del soggetto NIS o sui quali esercita il controllo, anche parziale. [solo soggetti essenziali]

IS-2

Il soggetto ha evidenza della divulgazione non autorizzata o abusiva, all'esterno del soggetto NIS, di dati digitali di proprietà del soggetto NIS o sui quali esercita il controllo, anche parziale.

IS-3

Il soggetto ha evidenza della divulgazione, all'esterno del soggetto NIS, di dati corrotti di proprietà del soggetto NIS o sui quali ne esercita il controllo, anche parziale.

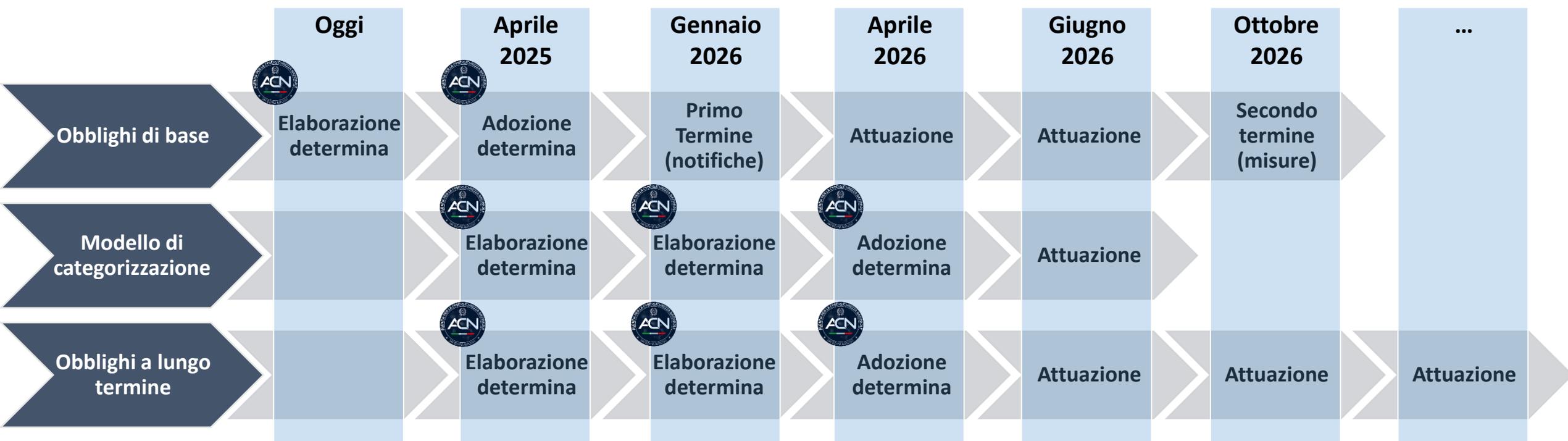
IS-4

Il soggetto ha evidenza della violazione del livello di servizio atteso dei servizi e/o delle attività del soggetto NIS, sulla base dei livelli di servizio atteso stabiliti dal soggetto NIS stesso.

Decreto Legislativo NIS (Gradualità)



Gradualità degli obblighi



Obblighi

- **Registrazione (articolo 7), Determinazione 38565/2024**
- Responsabilità dei vertici (articolo 23)
- Misure di sicurezza (articolo 24)
- Notifiche di incidente (articolo 25)
- Anche dati dei nomi di dominio (articolo 29)

Obblighi di base

- Obblighi, anche orizzontali, minimi per tutta l'infrastruttura con un orizzonte a breve termine

Obblighi a lungo termine

- Obblighi, anche settorializzati e potenzialmente ambiziosi, proporzionati in base alla categorizzazione e con scadenze a medio e lungo termine



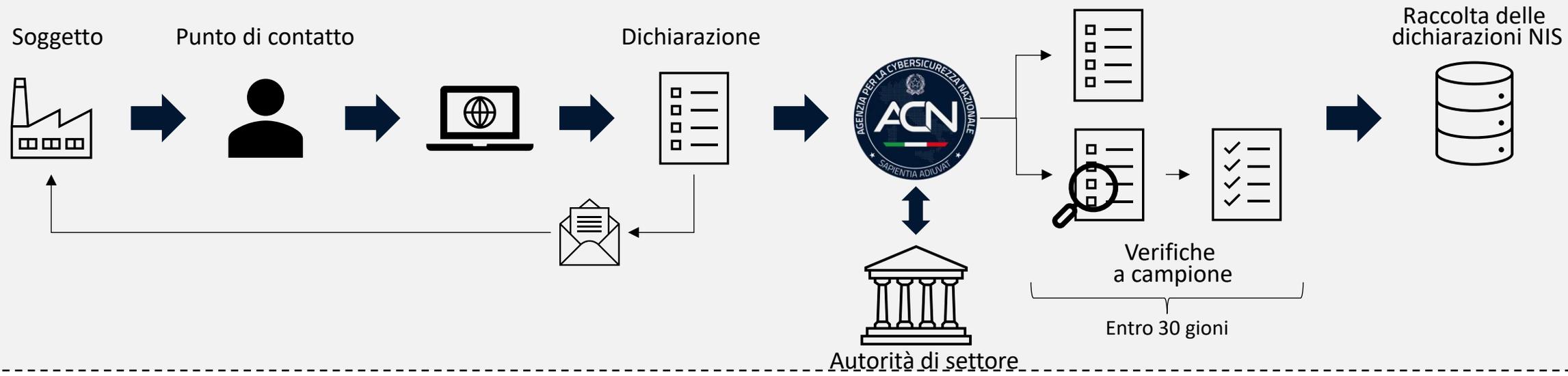
Decreto Legislativo NIS (Registrazione)



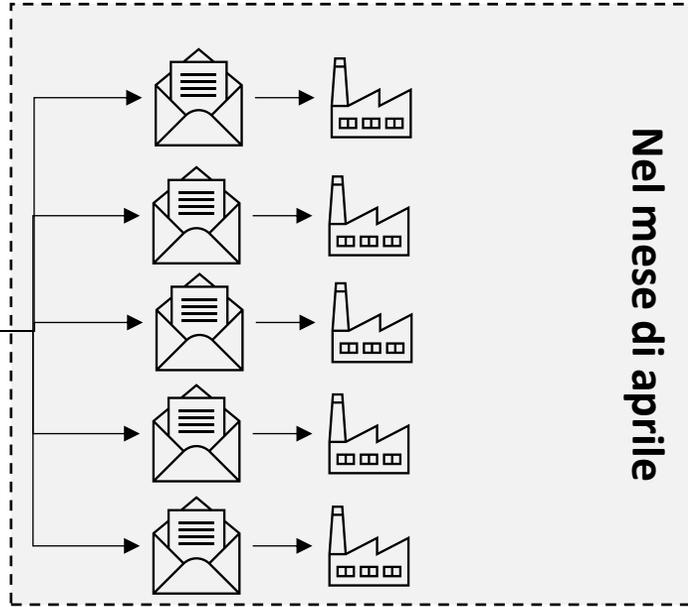
SCEGLIERE IL PUNTO DI CONTATTO

Verifiche di coerenza e costituzione dell'elenco dei soggetti NIS

Dal 1° dicembre al 28 febbraio



Entro il 31 marzo



Nel mese di aprile



Decreto Legislativo NIS (Attuazione)

Recepimento e attuazione

Recepimento (febbraio 23- metà ottobre 24)

- Avvio informale di alcuni tavoli settoriali
- Adozione definitiva in CDM (7 agosto)
- **Pubblicazione in Gazzetta Ufficiale (1° ottobre)**
- **Entrata in vigore (16 ottobre)**

Prima fase attuativa (metà ottobre 24 – metà aprile 25)

- [ACN e Autorità di settore] Avvio formale di tutti i tavoli settoriali
- [Soggetti] **Censimento e registrazione dei soggetti (entro febbraio 2025)**
- [ACN e Autorità di settore] **Adozione dell'elenco dei soggetti NIS e notifica (aprile 2025)**
- [ACN] **Elaborazione e adozione degli obblighi di base (aprile 2025)**

Seconda fase attuativa (metà aprile 25 – metà aprile 26)

- [Soggetti] **Implementazione obblighi di base (termine per notifiche di incidente 01/2026)**
- [ACN] Monitoraggio e supporto dell'implementazione obblighi di base
- [ACN] Elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
- [ACN] **Elaborazione e adozione degli obblighi a lungo termine (aprile 2026)**

Terza fase attuativa (da metà aprile 26)

- [Soggetti] **Completamento dell'implementazione obblighi di base (termine per misure di sicurezza 10/2026)**
- [Soggetti] Categorizzazione delle attività e dei servizi
- [Soggetti] Implementazione degli obblighi a lungo termine



Decreto Legislativo NIS (Materiale informativo)

NIS

Dal 16 ottobre 2024 è in vigore la nuova normativa Network and Information Security (NIS). ACN è l'Autorità competente NIS e punto di contatto unico.

[Scopri NIS](#)

La normativa

Registrazione

Domande frequenti

Ambito

Obblighi

Notizie ed eventi

Una nuova struttura è in vigore la nuova normativa Network and Information Security (Direttiva NIS) di derivazione europea.

Il recepimento della direttiva con il decreto legislativo del 4 settembre 2024, n. 138 ([decreto NIS](#)), mira a garantire l'aumento del livello di sicurezza informatica del tessuto produttivo e delle Pubbliche Amministrazioni del Paese, in armonia con gli altri Stati membri dell'Unione Europea.

L'Agencia per la cybersicurezza nazionale è l'Autorità competente NIS.

Dal 1° dicembre 2024 al 28 febbraio 2025, le medie e grandi imprese, in alcuni casi anche le piccole e microimprese, o le Pubbliche amministrazioni a cui si applica la nuova normativa devono registrarsi sul portale servizi ACN.

In seguito, si avvierà, ad aprile 2025, un percorso condiviso di rafforzamento della sicurezza informatica.

[Guarda il video](#)

[Leggi il decreto](#)

[Registrazione](#)



La normativa

L'impianto normativo rafforza quanto già previsto dal precedente quadro NIS, ampliandone il campo di applicazione e prevedendo un criterio omogeneo per l'identificazione dei soggetti.

La norma estende gli obblighi in materia di misure di sicurezza e di notifica degli incidenti, rafforza i poteri di supervisione, struttura maggiormente i meccanismi e gli organi preposti alla risposta agli incidenti e alla gestione della crisi. Introduce, infine, nuovi strumenti, come la divulgazione coordinata delle vulnerabilità.

Nella normativa sono contenute novità sulla gestione del rischio da parte degli operatori, che prevedono misure di sicurezza adeguate e un sistema di notifica degli incidenti efficace e reattivo. Inoltre, il decreto NIS favorisce la cooperazione e condivisione delle informazioni, attraverso diverse modalità di scambio, a livello sia nazionale che europeo. Al fine di promuovere l'applicazione concreta ed efficiente di una norma ambiziosa, il decreto NIS pone particolare enfasi sulle attività di supporto e sulla gradualità e proporzionalità degli obblighi normativi.

[Scopri di più](#)

Ambito di applicazione

Il campo di applicazione è ampliato a 18 settori, di cui 11 altamente critici (originariamente 8) e 7 critici (di nuova introduzione), interessando oltre 80 tipologie di soggetti pubblici e privati, incluse tante pubbliche amministrazioni.

Dal 1° dicembre 2024 al 28 febbraio 2025, le medie e grandi imprese, in alcuni casi anche le piccole e microimprese, a



[Home](#) / [Domande frequenti](#) / [NIS](#)

DOMANDE FREQUENTI

[PNRR](#)

[Cloud](#)

[NIS](#)

[PSAC](#)

[Canoni](#)

[CSIRT Italia](#)

NIS

Cerca nelle domande frequenti

Aspetti generali

- 1.1 Cos'è la nuova Direttiva NIS (Direttiva 2022/2555)?
- 1.2 Quando è entrata in vigore in Italia la nuova Direttiva NIS (Direttiva 2022/2555)?
- 1.3 Quali sono gli elementi fondanti della nuova normativa NIS?
- 1.4 Qual è l'Autorità nazionale competente NIS e quali funzioni svolge?
- 1.5 Quali sono le Autorità di settore NIS e quali funzioni svolgono?
- 1.6 Quali sono gli obblighi previsti dalla nuova normativa NIS e quando entreranno in vigore?
- 1.7 Quali sono le principali scadenze previste?
- 1.8 Cos'è EU-CyCLONe e che compiti svolge?

Ambito di applicazione

- 2.1 Quali sono i settori e i soggetti che ricadono nell'ambito di applicazione?
- 2.2 Che differenza c'è fra soggetti essenziali e importanti?
- 2.3 Come faccio a sapere se sono una grande, media o piccola impresa?
- 2.4 Le micro e piccole imprese rientrano nell'ambito di applicazione della nuova disciplina NIS?
- 2.5 Quali medie e grandi imprese rientrano nell'ambito di applicazione della nuova disciplina NIS?
- 2.6. Quali pubbliche amministrazioni rientrano nell'ambito di applicazione della nuova disciplina NIS?
- 2.7. Quali organizzazioni del settore pubblico rientrano nell'ambito di

