Attuazione del decreto NIS
I prossimi passi

03/02/2025

Direttiva NIS2

(Principi generali)

Direttiva NIS2 – 2022/2555

Estensione ambiti di applicazione

- **18 settori: 11 settori altamente critici** (originariamente 8) e **7 settori critici** (originariamente 0)
- **Intera infrastruttura ICT** (originariamente solo reti e sistemi serventi i servizi essenziali)

Processo di identificazione dei soggetti

- **Soggetti** distinti tra entità **essenziali e importanti**
- **Identificazione automatica** sulla base di criteri oggettivi (da **media imprese in su**, salvo eccezioni)
- L'Autorità ha anche la facoltà di identificare ulteriori soggetti

Rafforzamento degli obblighi

- Misure di sicurezza specifiche e **proporzionate rispetto al rischio** posto al sistema informativo e di rete
- Approccio **multi-rischio** (coordinamento con Direttiva CER)
- Processo di notifica più dettagliato
- Poteri di esecuzione, ispettivi e sanzionatori rafforzati (**allineamento alle sanzioni GDPR**)

Nuovi strumenti

- **Divulgazione coordinata delle vulnerabilità (CVD)**
- **Cyber crisis liaison organisation network** (CyCLONe) e Autorità nazionale competente per la gestione delle crisi informatiche
- Revisione tra pari e mutua assistenza

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**	**Importanti[1]**	**Fuori ambito[2]**
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**		

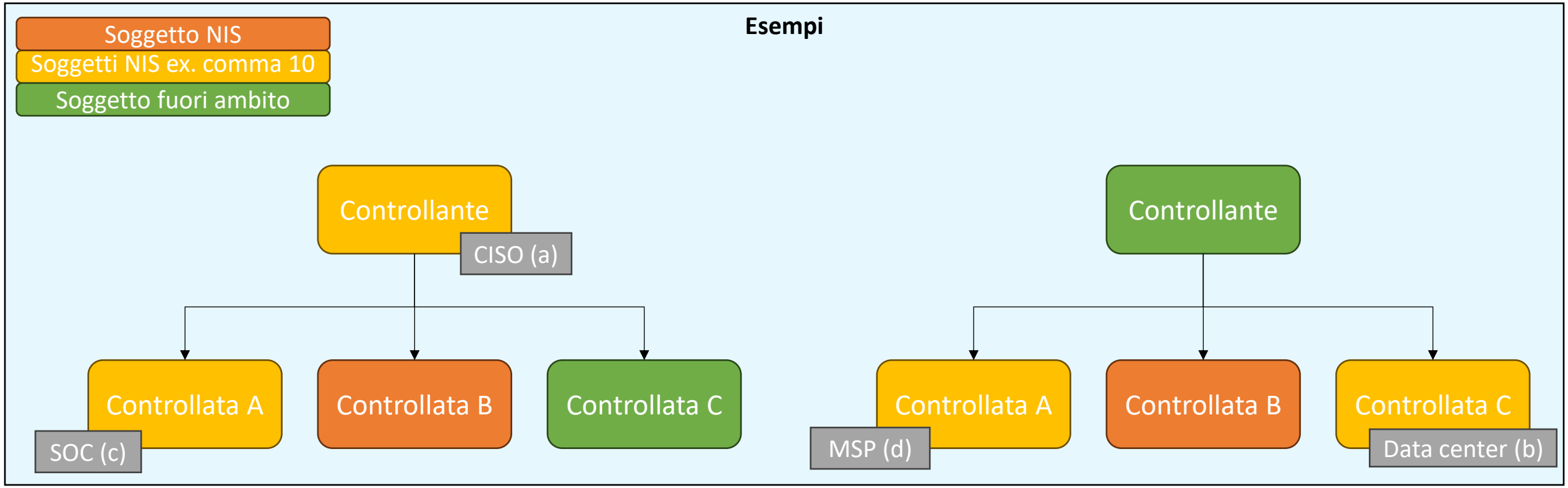
Settori, sottosettori e tipologie di soggetti introdotti dalla NIS2

Approfondimento sull'ambito di applicazione – Imprese collegate/associate/gruppi

ARTICOLO 3, comma 10 – Ambito di applicazione

Il comma 10 dell'articolo 3 attrae nell'ambito di applicazione le organizzazioni (persona giuridiche) di un gruppo che possono avere un impatto in termini di processi decisionali o tecnici su soggetti NIS (nazionali) del medesimo gruppo, ovvero soddisfano i seguenti criteri:

a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto NIS;
b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto NIS;
c) effettua operazioni di sicurezza informatica del soggetto NIS;
d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto NIS.



Giurisdizione (articolo 5)

Il decreto NIS si applica alle singole organizzazioni (persone giuridiche) e non ai gruppi di imprese

Organizzazioni stabilite sul territorio nazionale

- Regola generale

Organizzazioni che offrono servizi sul territorio nazionale

- Fornitori di reti pubbliche di comunicazione elettronica e fornitori di servizi di comunicazione elettronica accessibili al pubblico

Organizzazioni con lo stabilimento principale o il rappresentante in UE in Italia

- fornitori di servizi di sistema dei nomi di dominio DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network

Sono stabiliti sul territorio nazionale e non hanno stabilimenti in altri Stati membri, anche qualora abbiano stabilimenti al di fuori dell'Unione europea

Hanno stabilimenti in più Stati membri e sul territorio nazionale è presente lo stabilimento principale, individuato ai sensi dell'articolo 5, comma 2

Non hanno alcun stabilimento nell'Unione europea, offrono i loro servizi sul territorio nazionale e, ai sensi dell'articolo 5, comma 3, hanno designato il rappresentante nell'Unione in Italia.

Decreto Legislativo NIS (Governance)

Autorità e Tavolo per l'attuazione della disciplina NIS

Autorità nazionale competente NIS
Autorità di settore NIS
Altri membri del tavolo

Agenzia per la cybersicurezza nazionale

PCM

MEF

MIMIT

MASAF

MASE

MIT

MUR

MIC

MSAL

Conferenza permanente

per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano

Autorità di settore NIS e Tavoli di settore (articolo 11)

Autorità di settore NIS

- **Verificano l'elenco dei soggetti NIS**
- **Supportano l'individuazione dei soggetti essenziali e dei soggetti importanti**
- Individuano i soggetti a cui si applicano le deroghe di cui all'articolo 3, comma 4;
- Supportano le funzioni e le attività di regolamentazione
- Elaborano dei contributi per la relazione annuale
- **Istituiscono e coordinano i tavoli settoriali**, al fine di contribuire **all'efficace e coerente attuazione settoriale** del decreto NIS nonché al relativo **monitoraggio**.
- Partecipano alle attività settoriali del Gruppo di Cooperazione NIS

Tavoli di settore

- **Camera di compensazione e confronto con i settori/soggetti NIS** per una efficace attuazione della disciplina
- Individuazione di criticità e condivisione di approcci in fase legislativa e regolamentare
- Monitoraggio dell’attuazione

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

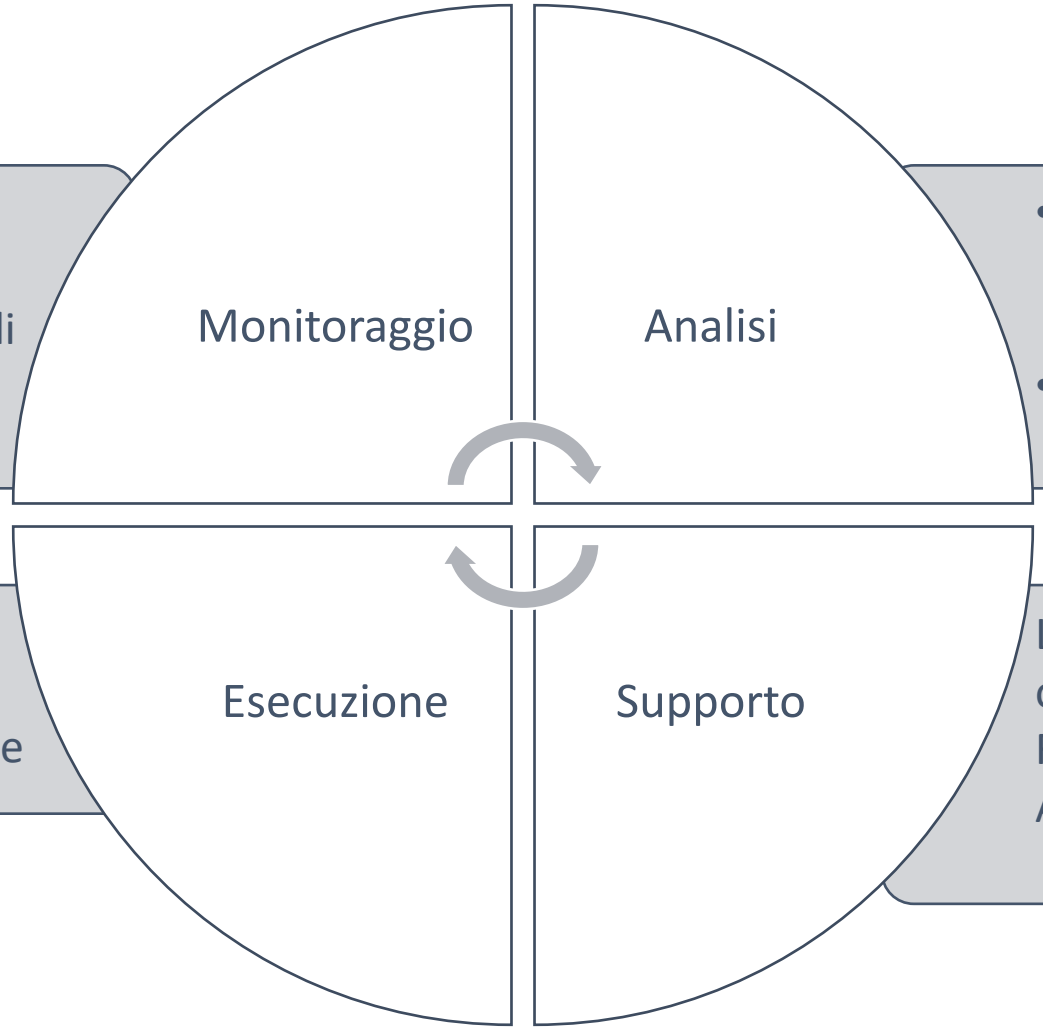
- Mancata registrazione, comunicazione dei dati, osservanza degli obblighi relativi agli obblighi relativi alle certificazioni, alla registrazione dei nomi di dominio e alle previsioni settoriali specifiche
- Sanzioni pecuniarie fino a 0,1% per soggetti essenziali e fino a 0,07% per soggetti importanti

Maggiorazione per reiterazione e sanzioni accessorie (anche per le persone fisiche)

Strumenti deflattivi del contenzioso

Regime più favorevole per la PA

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



- Acquisizione dello stato di attuazione degli obblighi
- Anche tramite il Tavolo NIS, i Tavoli settoriali e rendicontazioni periodiche

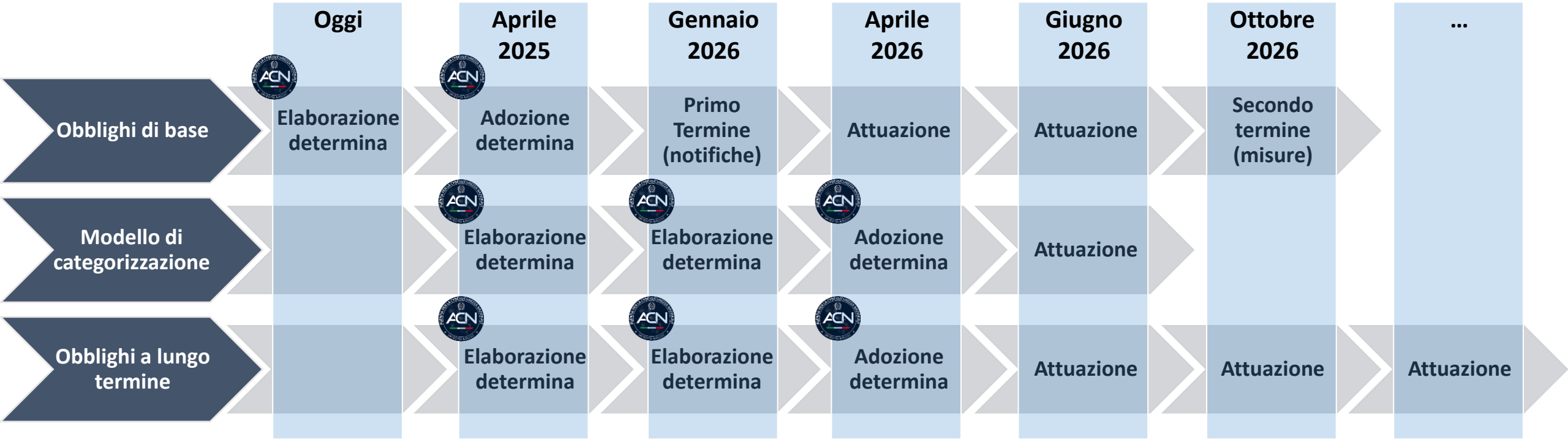
- Individuazione di criticità e soluzioni, sistemiche o individuali
- Anche tramite il Tavolo NIS e i Tavoli settoriali

Imporre audit di terze parti
Disporre di attuare istruzioni vincolanti o di porre rimedio a carenze

Linee guida, raccomandazioni e orientamenti non vincolanti
Richiesta di audit di terze parti
Avvertimenti

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)
- Banche 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)

Il Punto di contatto

Criteri generali

- Il Punto di contatto è il rappresentante legale o un suo procuratore generale oppure un dipendente delegato del soggetto.
- Salvo eccezioni è quindi un ruolo interno al soggetto NIS
- Riferisce direttamente al vertice gerarchico del soggetto NIS nonché agli organi di amministrazione e direttivi del soggetto medesimo ai fini di quanto previsto dal decreto NIS
- Non vi sono requisiti in relazione alle competenze

Deroghe

- PA: è possibile designare il dipendente di un'altra pubblica amministrazione soggetto NIS
- Gruppi di imprese: è possibile designare il dipendente di un altro soggetto NIS (nazionale) del medesimo gruppo
- Soggetti NIS extra-UE: è possibile designare dipendenti del rappresentante nell'UE in Italia

Responsabilità

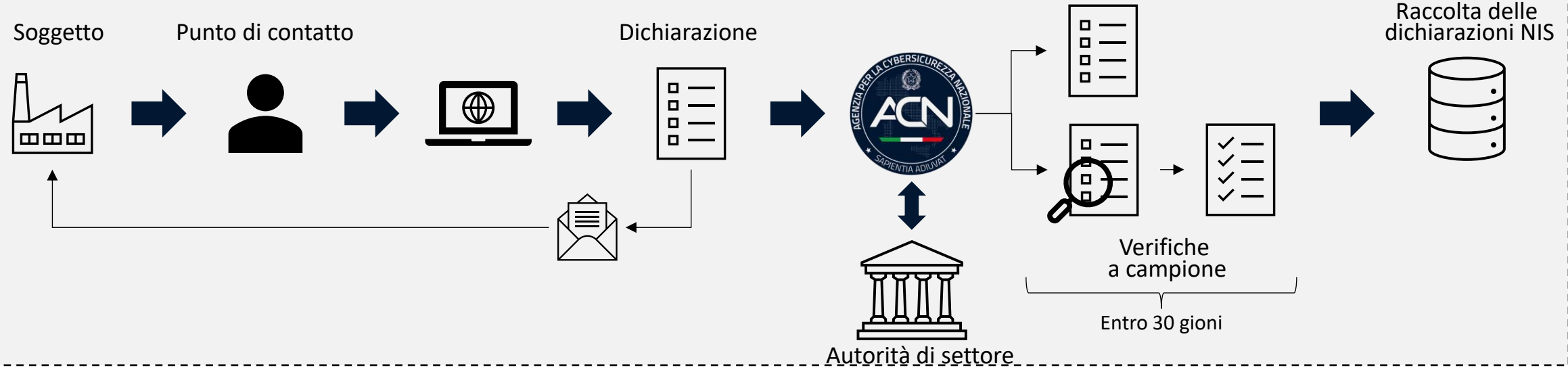
- "Cura" l'attuazione delle previsioni del decreto NIS presso il soggetto.
- Ai sensi degli articoli 23 e 38 del Decreto NIS, in prima battuta, la responsabilità delle violazioni è posta in capo ai vertici aziendali

Supporto

- Il Punto di contatto ha la facoltà di essere supportato anche da personale esterno
- Nei prossimi giorni, i Punti di contatto saranno abilitati a indicare un ulteriore utente per supportarlo nella compilazione (non sottoposizione) della dichiarazione

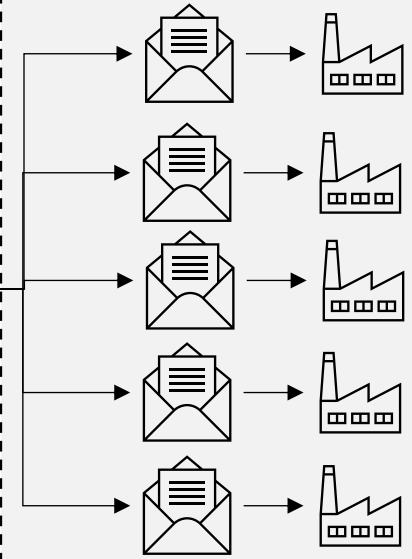
Verifiche di coerenza e costituzione dell'elenco dei soggetti NIS

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


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT