Attuazione del decreto NIS
I prossimi passi

30/01/2025

Direttiva NIS2 – 2022/2555

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**	**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

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

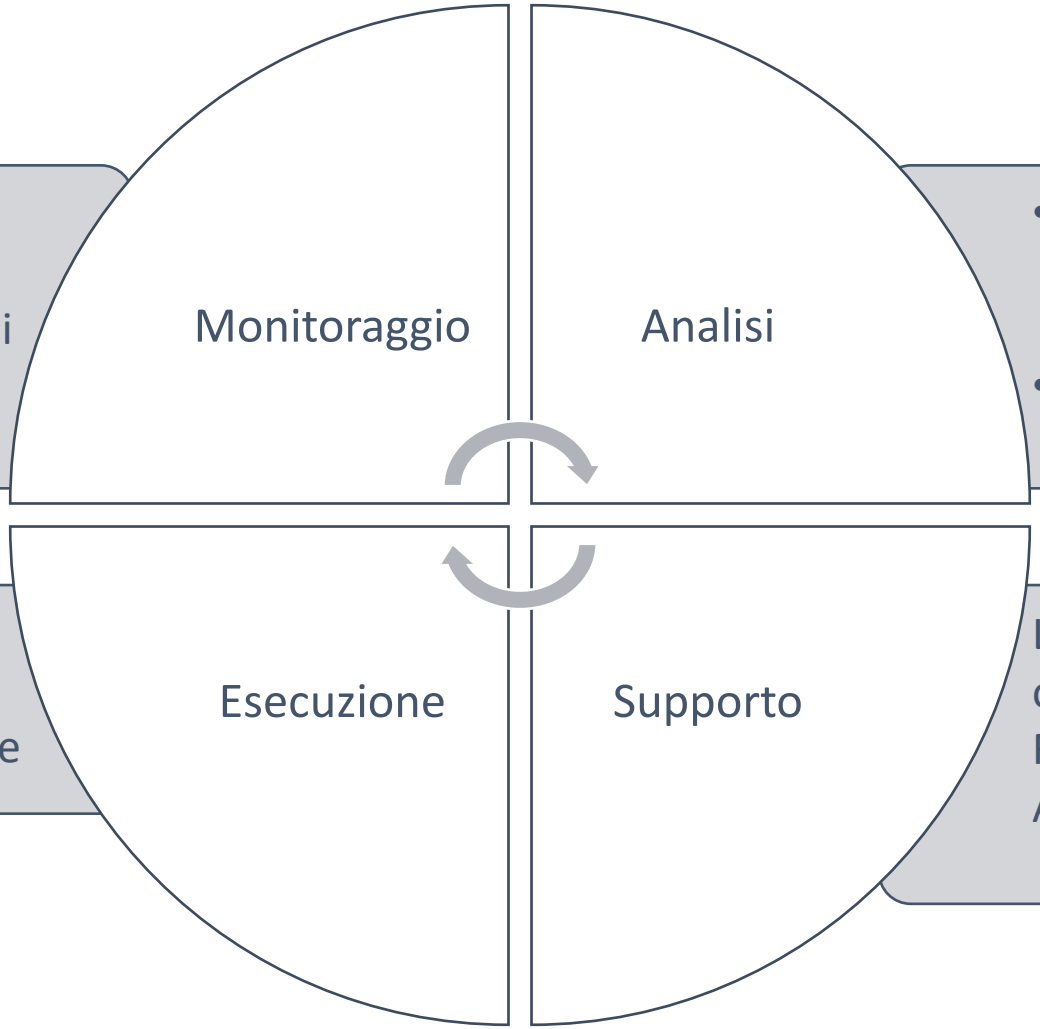
Altre violazioni

- 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)

- 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

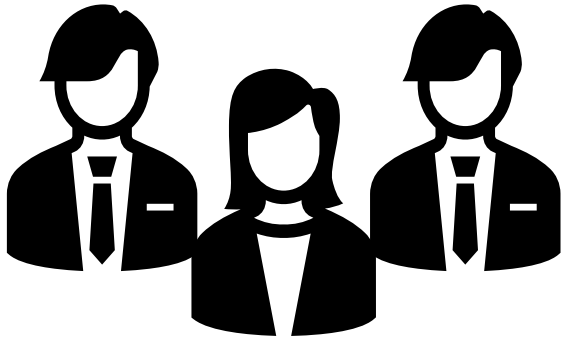
Linee guida, raccomandazioni e orientamenti non vincolanti
Richiesta di audit di terze parti
Avvertimenti

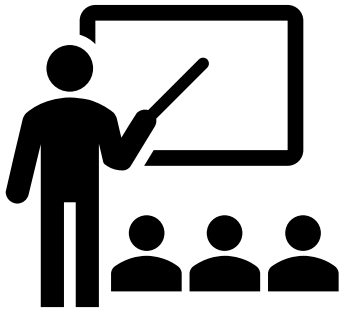
Decreto Legislativo NIS
(Vertici aziendali)

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

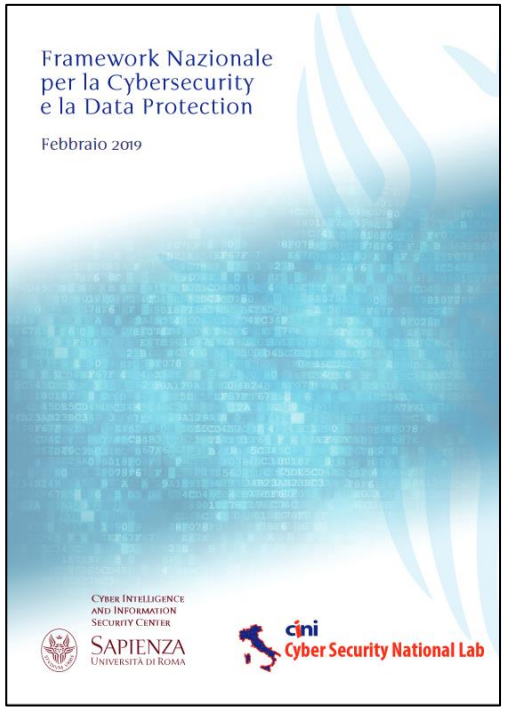
Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza

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

Misure di sicurezza

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

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: 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 verifichino 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.		●

Specifiche requisiti

Decreto Legislativo NIS
(Notifica di incidente)

Notifiche di incidente

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

NOTIFICHE VOLONTARIE POSSIBILI FIN DA SUBITO

Tassonomia incidenti

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]

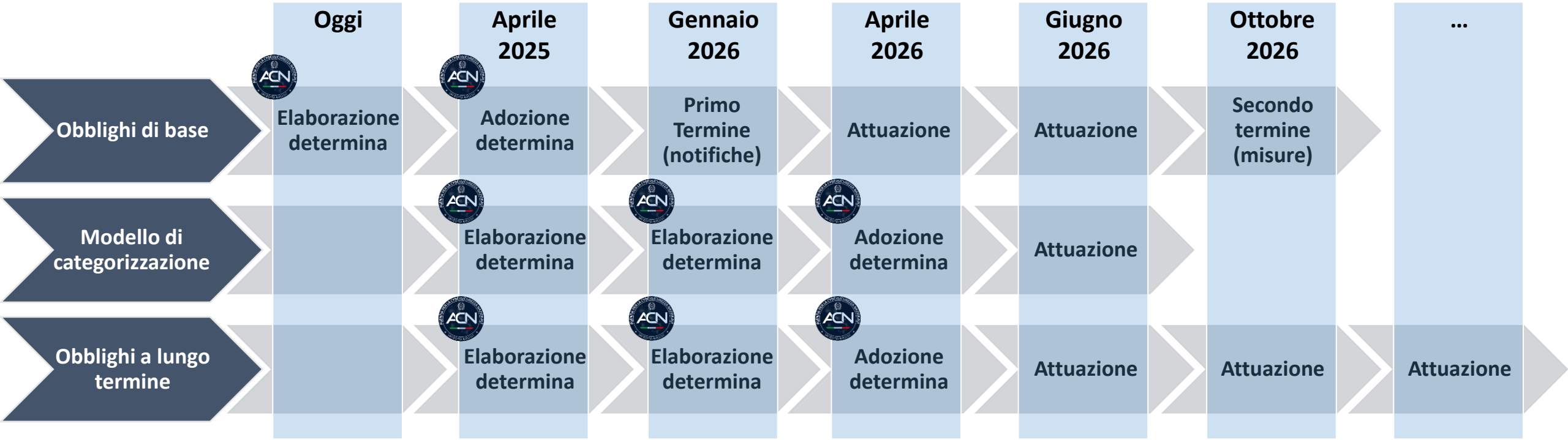
IS-2 Il soggetto ha evidenza della divulgazione non autorizzata o abusiva, all'esterno del soggetto NIS, di dati digitali di proprietà del soggetto NIS o sui quali esercita il controllo, anche parziale.

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)
- 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

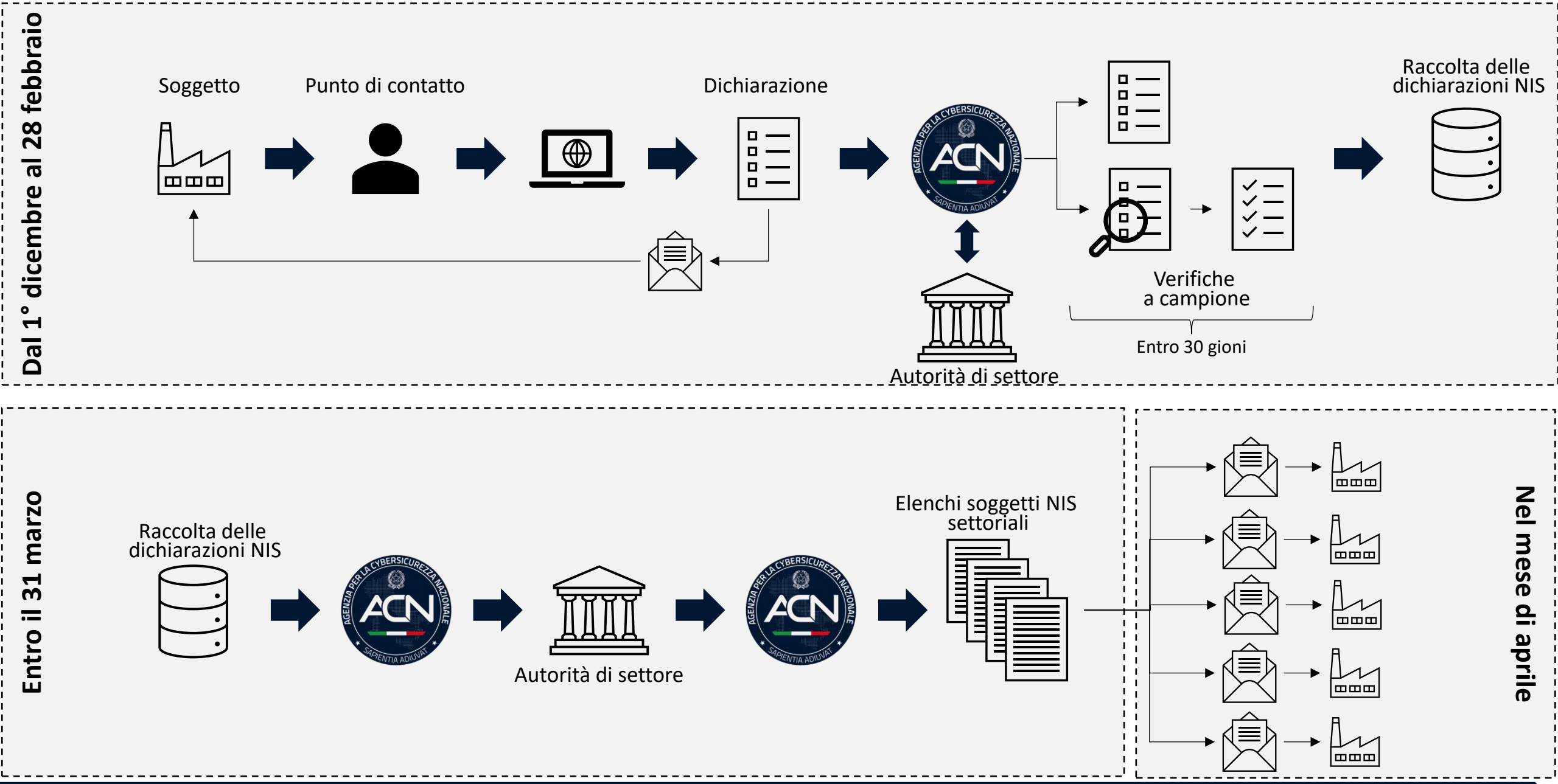
Obblighi a lungo termine

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

Decreto Legislativo NIS (Registrazione)

SCEGLIERE IL PUNTO DI CONTATTO

Verifiche di coerenza e costituzione dell'elenco dei soggetti NIS



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)

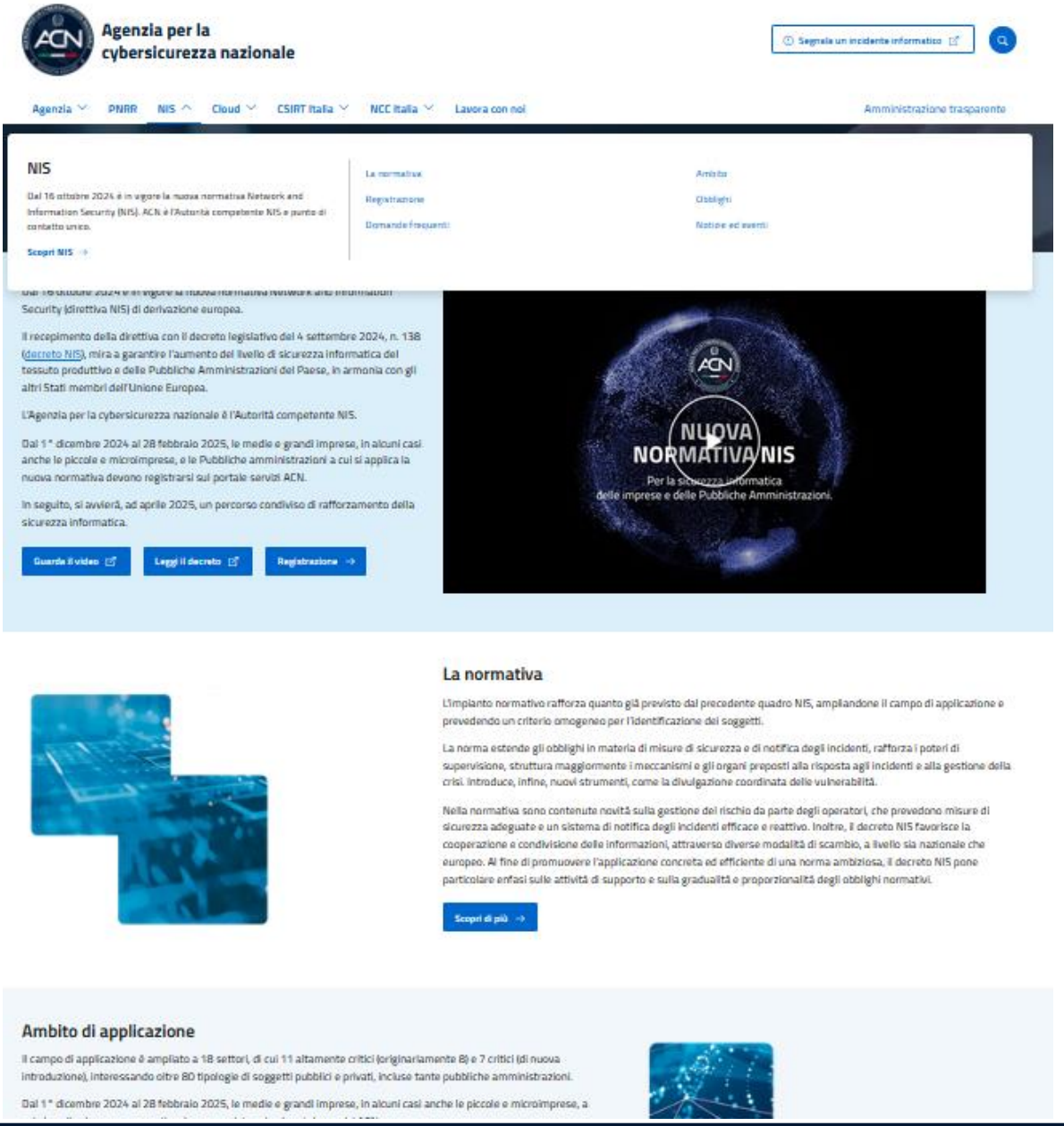
- [**Soggetti**] **Implementazione obblighi di base (termine per notifiche di incidente 01/2026)**
- [ACN] Monitoraggio e supporto dell'implementazione obblighi di base
- [ACN] Elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
- [ACN] **Elaborazione e adozione degli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

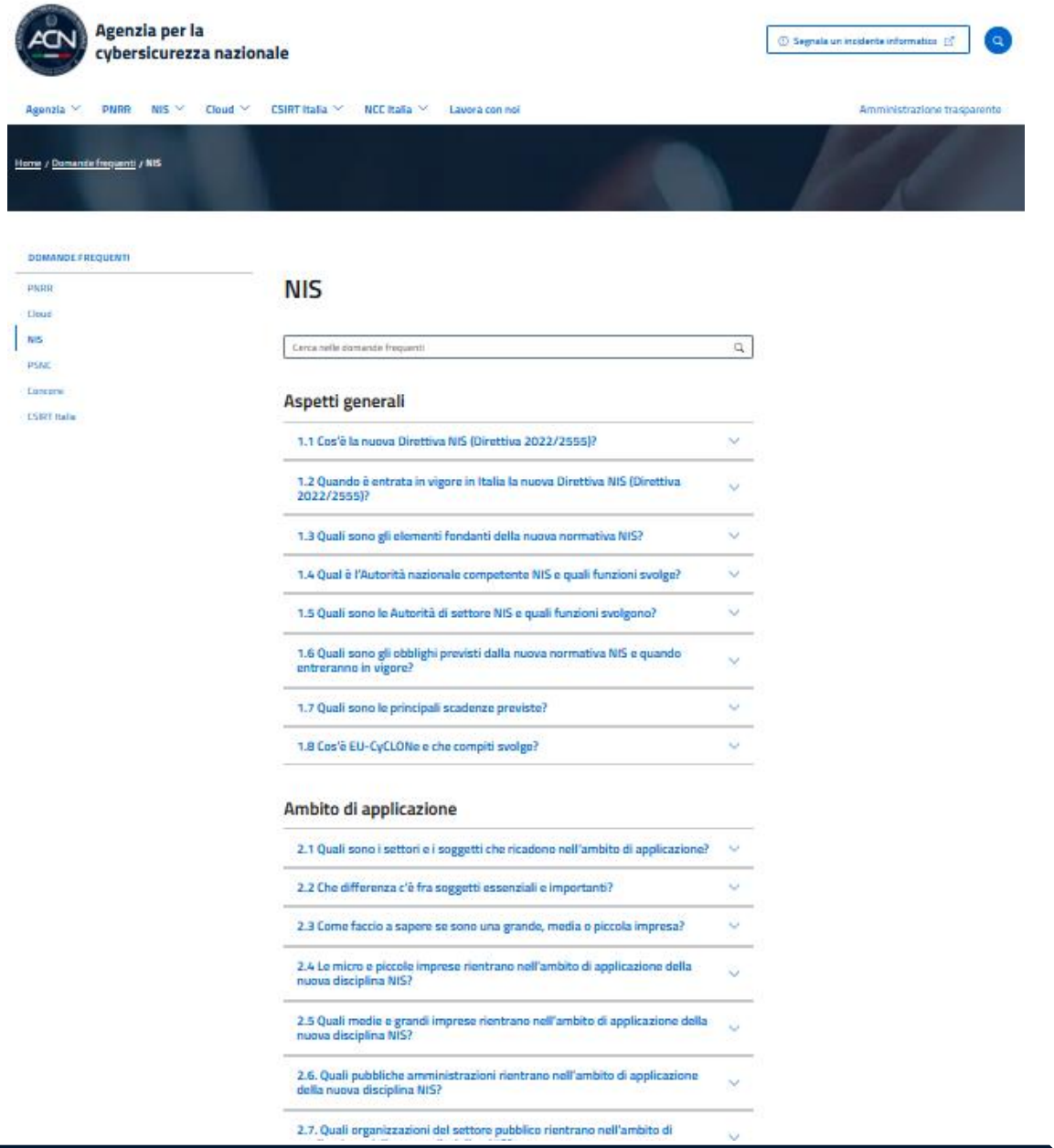
Terza fase attuativa
(da metà aprile 26)

- [**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)

acn.gov.it/nis






AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT