Il Decreto Legislativo n. 138/2024 e il recepimento della Direttiva (UE) 2022/2555 (“NIS 2”)

Obbligo di notifica (art. 25 decreto NIS

Base giuridica

D.Lgs. 138/2024 (decreto NIS)

Art. 23
Organi di amministrazione e direttivi

Art. 24
Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica

Art. 25
Obblighi in materia di notifica di incidente

Art. 31
Proporzionalità e gradualità degli obblighi

Art. 40
Attuazione

Art. 42
Fase di prima applicazione

Det. ACN obblighi di base

Allegato 1
Misure di sicurezza di base soggetti importanti

Allegato 2
Misure di sicurezza di base soggetti essenziali

Allegato 3
Incidenti significativi di base soggetti importanti

Allegato 4
Incidenti significativi di base soggetti essenziali

Incidenti significativi di base (1/2)

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 di 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.

Soggetti importanti ed essenziali
3 tipologie di incidenti

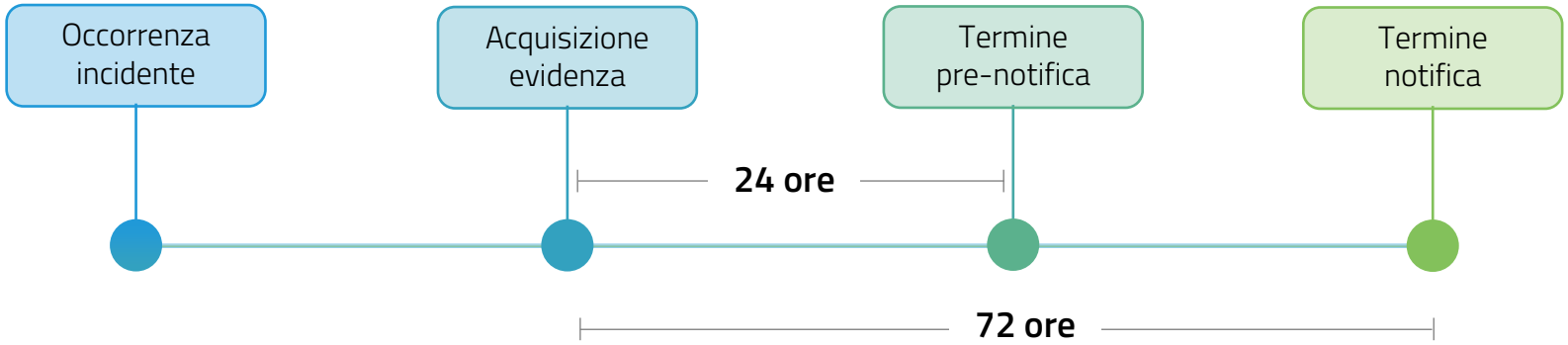
Solo soggetti essenziali
1 tipologia di incidente

Incidenti significativi di base (2/2)

Evidenza dell'incidente

Ai fini dell'adempimento dell'obbligo di notifica degli incidenti ciò che rileva è che il soggetto abbia evidenza del verificarsi di una delle tipologie di incidente indicate.

L'acquisizione dell'evidenza definisce il momento dal quale decorre il termine per l'obbligo di notifica.



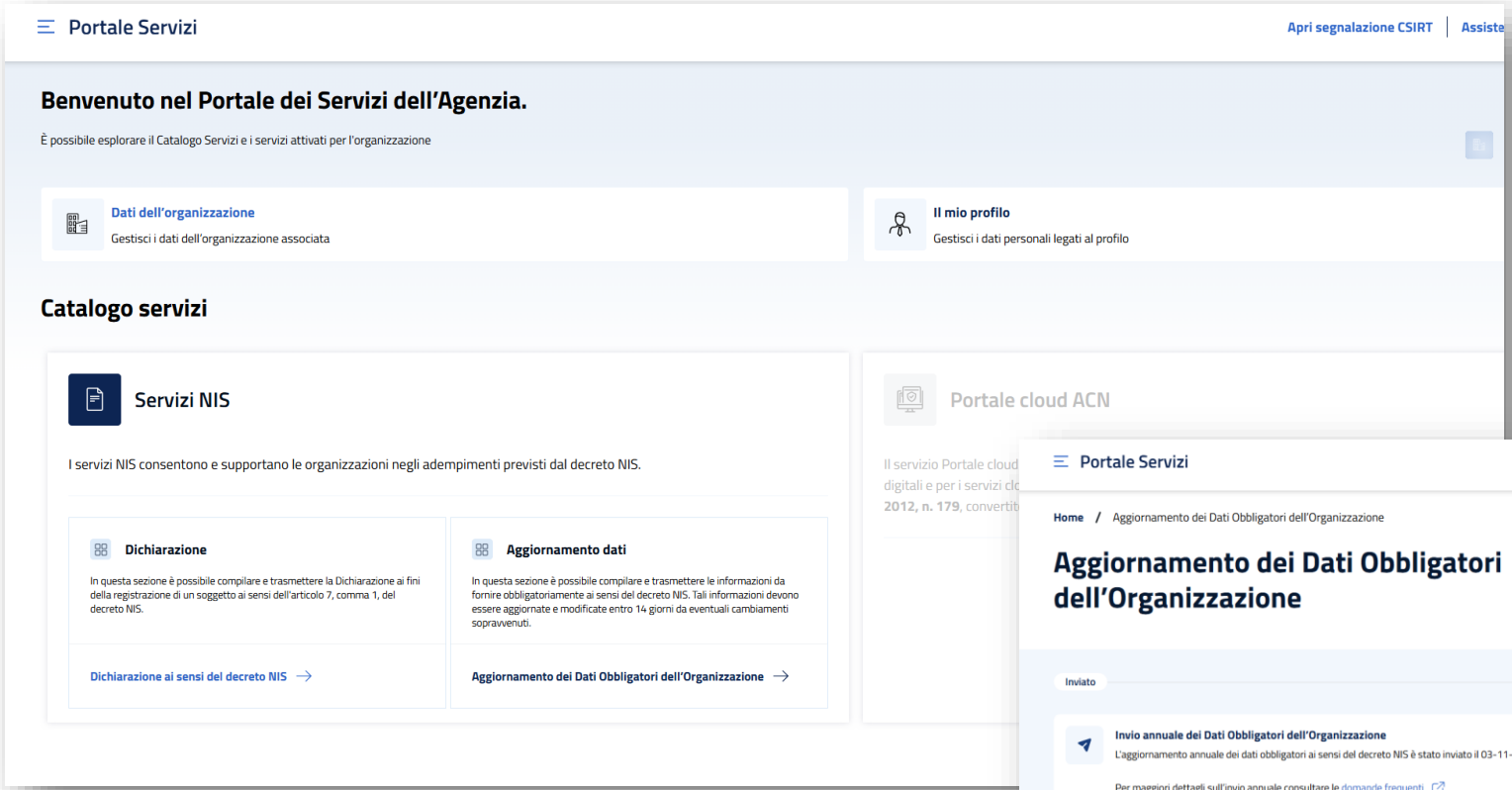
Abuso dei privilegi concessi

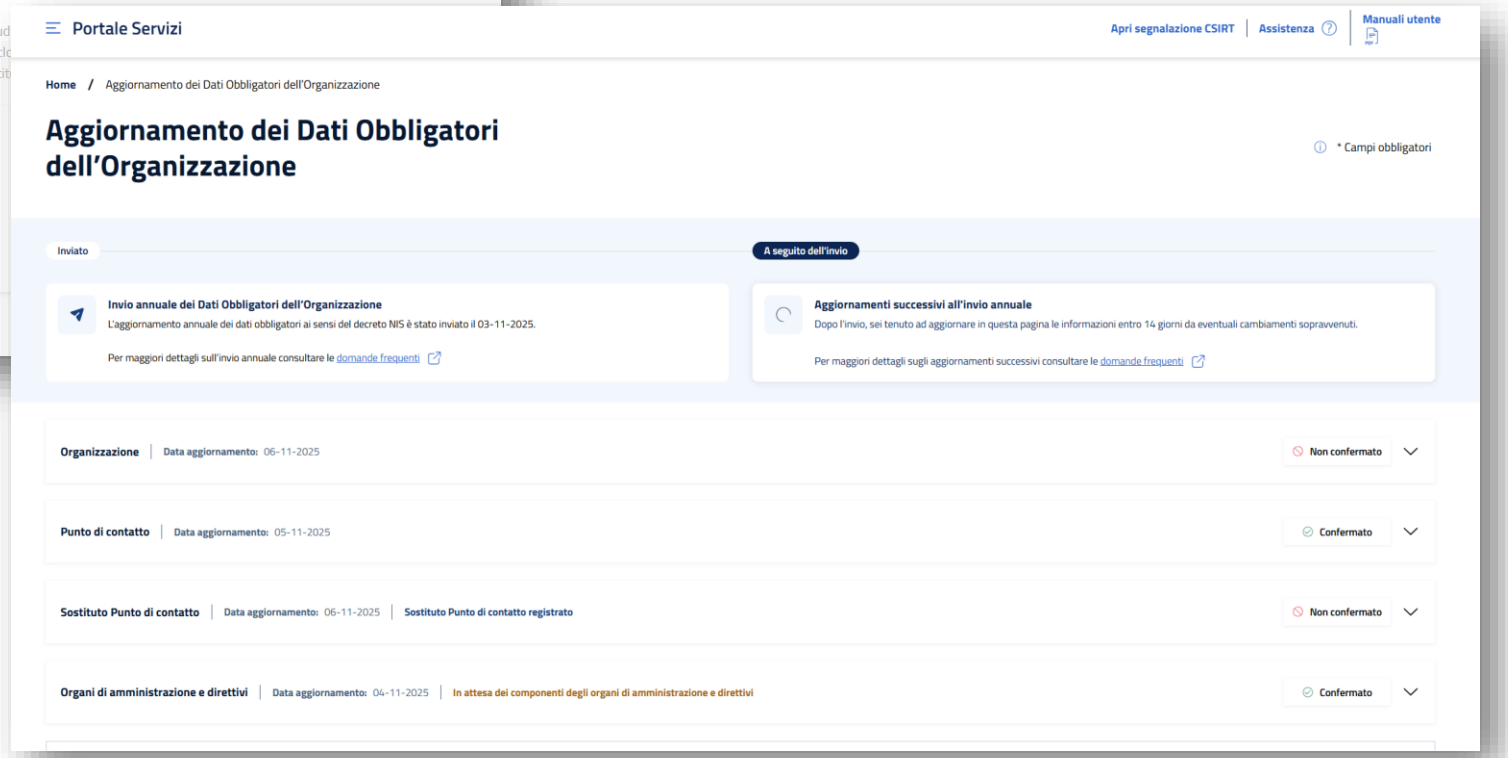
Fattispecie in cui un operatore abbia l'autorizzazione tecnica (ossia la disponibilità di credenziali che sono configurate per accedere ai dati) per accedere a determinati dati ma tale acceso sia effettivamente illecito in quanto, ad esempio, effettuato in violazione delle politiche del soggetto o risulti strumentale al perseguimento di scopi estranei alle necessità funzionali di accesso..

Referente CSIRT

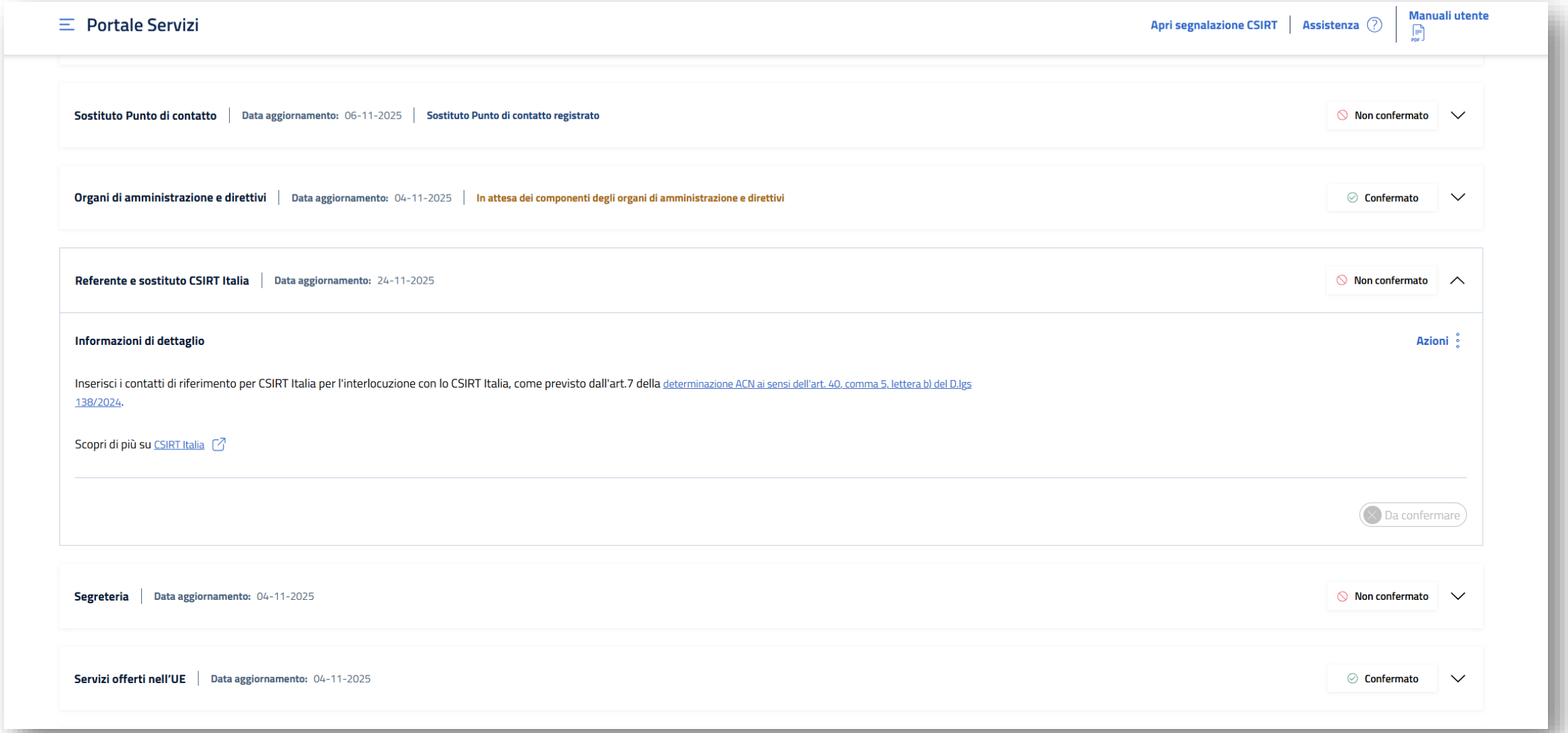
- Introdotto dalla determinazione ACN 333017/2025.
- Interloquisce con lo CSIRT Italia ed effettua le notifiche obbligatorie e volontarie
- Può essere coadiuvato da sostituti referenti CSIRT
- Possibile individuare personale esterno al soggetto (auspicabile però che si a interno)

Inserimento dati (1/3)

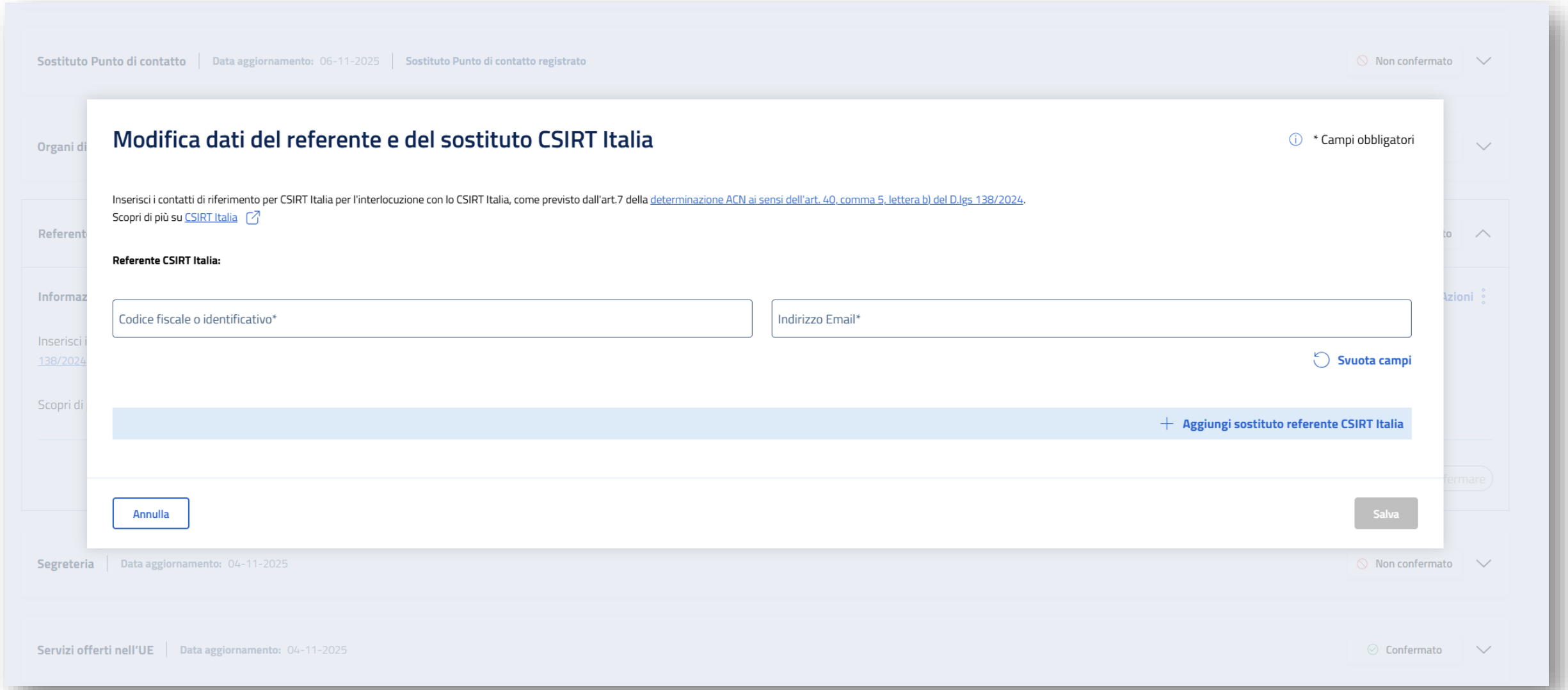




Inserimento dati (2/3)

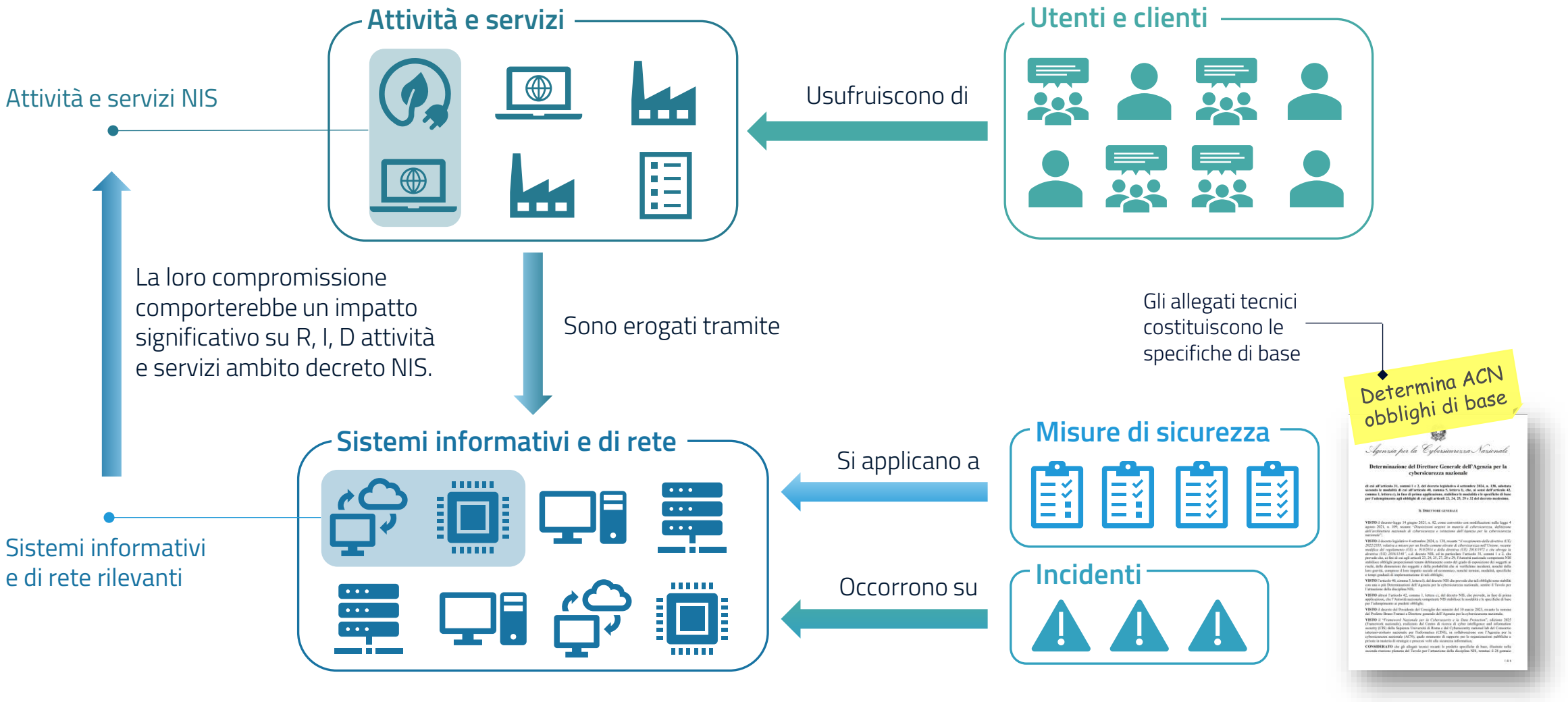


Inserimento dati (3/3)



Misure di sicurezza e gestione del rischio in ambito NIS

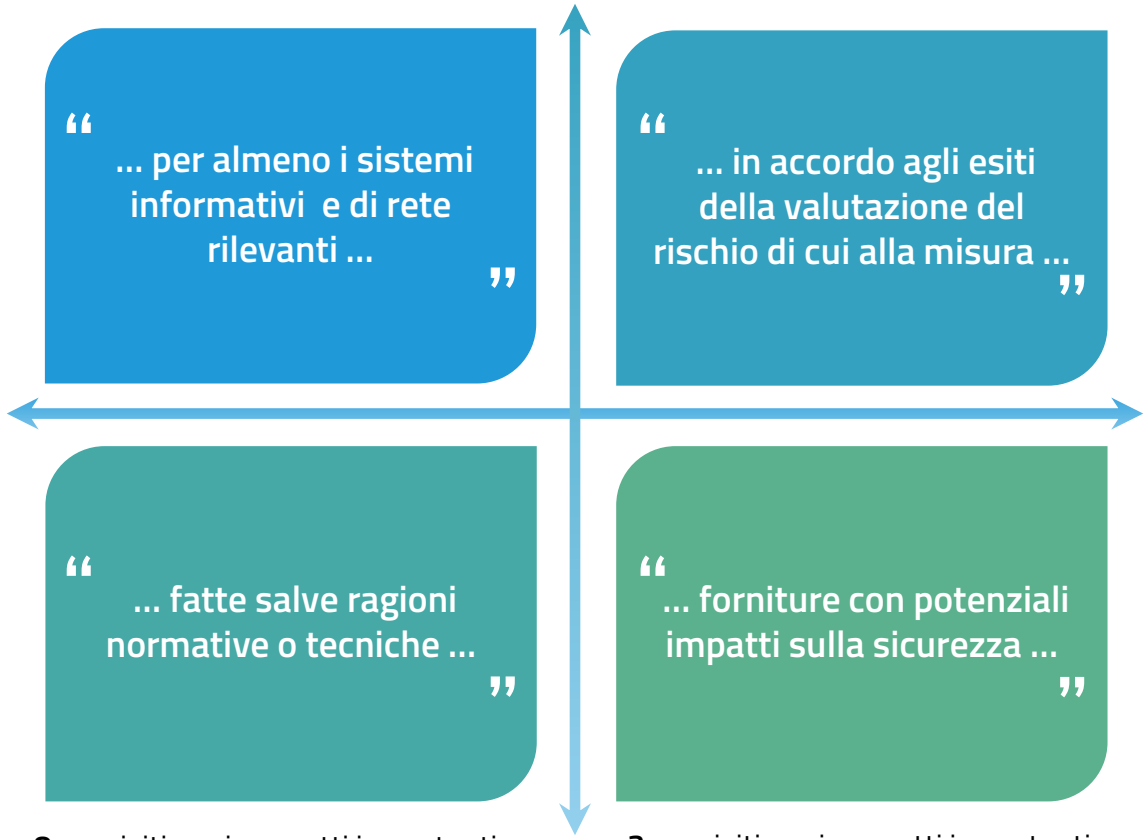
Modello concettuale



Approccio basato sul rischio (1/2)

Ambito	Livello di rischio	Proporzionalità	Approccio	Clausole
Le misure di sicurezza si applicano a tutti i sistemi informativi e di rete del soggetto.	Ogni sistema informativo e di rete è caratterizzato da un proprio livello di rischio.	L'art. 31 del decreto prevede che si tenga conto, nello stabilire gli obblighi, del grado di esposizione dei soggetti ai rischi.	Le misure di sicurezza sono state sviluppate secondo un approccio basato sul rischio.	Previsione per i requisiti di maggiore complessità di specifiche clausole.

Approccio basato sul rischio (2/2)



Facoltà di limitare l'ambito di applicazione per specifici requisiti ai sistemi informativi di rete la cui compromissione determina un impatto significativo su R, I, D per i servizi e le attività per i quali il soggetto rientra nell'ambito di applicazione del decreto NIS

Possibilità di adattare le modalità di attuazione di specifici requisiti sulla base degli esiti della valutazione del rischio.

Deroga all’applicazione del requisito se sussistono vincoli normativi (ad esempio, leggi o regolamenti) o tecnici (ad esempio, limiti tecnologici o operativi) che non ne permettano l’implementazione

Sono considerate le forniture la cui eventuale compromissione può determinare effetti sulla sicurezza dei sistemi informativi e di rete.

Esempio misura di sicurezza di base

PR.DS-11

I backup dei dati sono creati, protetti, mantenuti e verificati.

PUNTO	REQUISITO	S_I	S_E
1	In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●
3	Per almeno i sistemi informativi e di rete rilevanti, è assicurata la riservatezza e l'integrità delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.		●
4	Per almeno i sistemi informativi e di rete rilevanti, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.		●
5	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 3 e 4.		●

Misure di sicurezza e valutazione del rischio

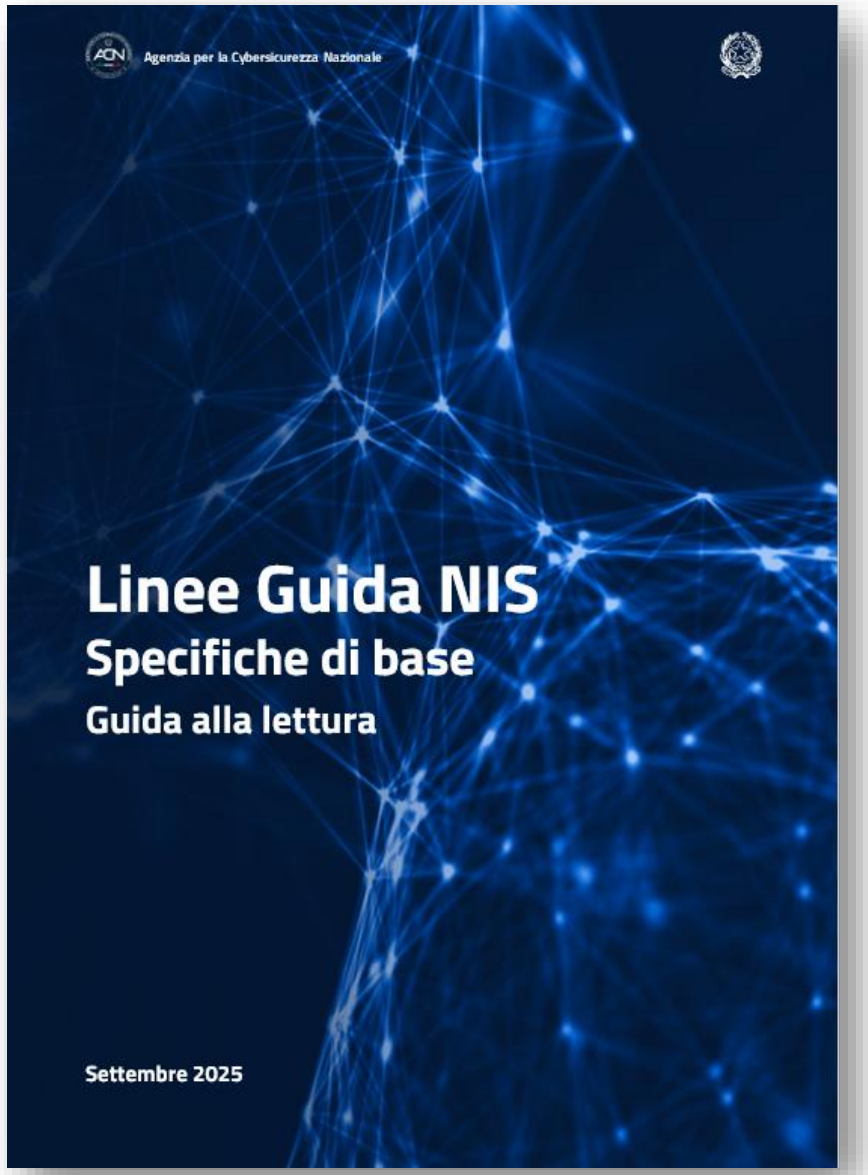
Definizione delle misure di sicurezza

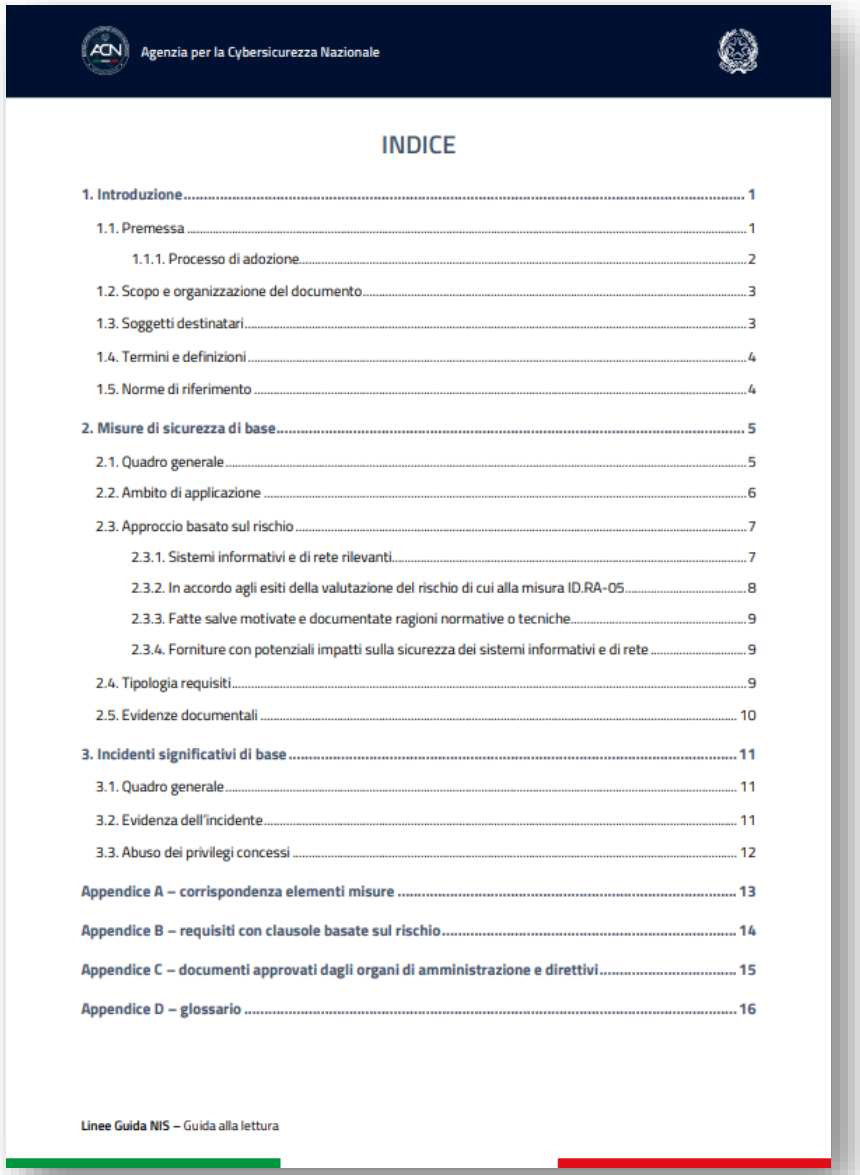
- Nel definire le misure di sicurezza si possono adottare due tipi di approcci: *basato su accountability o prescrittivo.*
- In considerazione delle peculiarità della disciplina NIS (in particolare dell'articolo 31), le misure di sicurezza sono state sviluppate adottando un approccio ibrido basato sul rischio (per i requisiti di maggiore complessità previste specifiche clausole).

Finalità della valutazione del rischio

- Fornisce consapevolezza ai soggetti.
- Definisce le modalità di attuazione (*dove* e *come*) dei requisiti in cui è presente la clausola *… in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05* (5 per i soggetti essenziali, 8 per quelli importanti).
- Informa le modalità di implementazione delle misure di sicurezza (ad es. misure per l'accesso remoto, contenuti del piano di formazione, ecc.).

Guida alla lettura




Agenzia per la Cybersicurezza Nazionale

INDICE

Prossimi passi

Recepimento e attuazione

Febbraio 23 - metà ottobre 24

Recepimento

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

Metà ottobre 24 - metà aprile 25

Prima fase attuativa

- [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)**

Metà aprile 25 - metà ottobre 26

Seconda fase attuativa

- **[Soggetti] Aggiornamento annuale** (termine 07/2025)
- **[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)**

Da metà aprile 26

Terza fase attuativa

- **[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

Gradualità degli obblighi

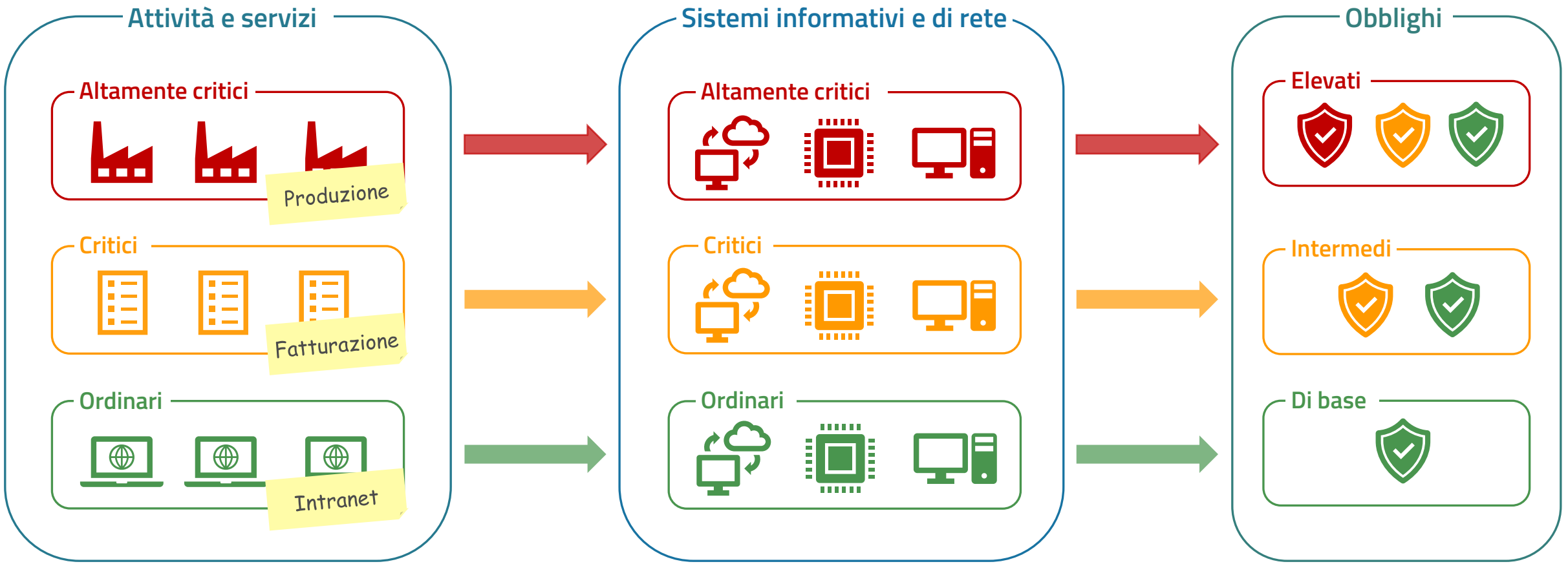
Specifiche di base

Specifiche degli obblighi, anche orizzontali, minimi per tutta l'infrastruttura con un orizzonte a breve termine.

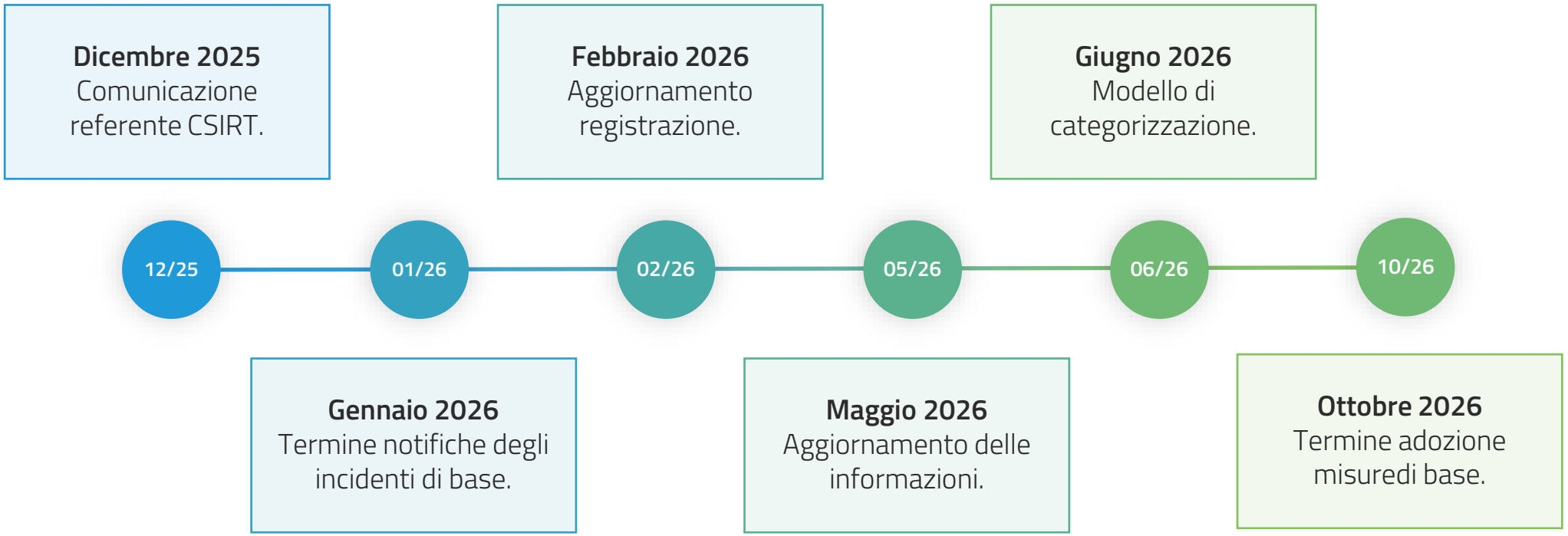
Specifiche a lungo termine

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

Proporzionalità degli obblighi



Scadenze


Dicembre 2025
Comunicazione referente CSIRT.
Febbraio 2026
Aggiornamento registrazione.
Giugno 2026
Modello di categorizzazione.
12/25
01/26
02/26
05/26
06/26
10/26
Gennaio 2026
Termine notifiche degli incidenti di base.
Maggio 2026
Aggiornamento delle informazioni.
Ottobre 2026
Termine adozione misuredi base.

https://www.acn.gov.it/portale/nis

https://www.acn.gov.it/portale/nis/registrazione

https://www.youtube.com/watch?v=ikC4PPTIxJM

https://www.acn.gov.it/portale/faq/nis

https://portale.acn.gov.it/