



Tavolo settoriale MSAL

Ordine del giorno

1

Saluto del Direttore generale dell'UMPNNRR e apertura dei lavori

2

Introduzione e agenda della riunione

3

Punto della situazione sull'attuazione della disciplina NIS e sulle prossime scadenze

4

Giro di tavolo sullo stato di attuazione della disciplina NIS, con confronto sulle principali evidenze, eventuali criticità e aspetti di particolare interesse

5

Presentazione delle misure di sicurezza rafforzate e delle relative modalità di raccolta dei riscontri

6

Giro di tavolo e confronto sulle misure di sicurezza rafforzate, prime impressioni ed eventuali elementi di interesse emersi

7

Chiusura dei lavori

Saluto del Direttore generale dell'UMPNRR e apertura dei lavori

Primo punto all'ordine del giorno



Introduzione e agenda della riunione

Secondo punto all'ordine del giorno



Punto della situazione sull'attuazione della disciplina NIS e sulle prossime scadenze

Terzo punto all'ordine del giorno



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 D.lgs., 138/2024 (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 aprile 26

Seconda fase attuativa

- [Soggetti] **Aggiornamento annuale** (termine 07/2025)
- [Soggetti] **Implementazione obblighi di base** (termine per notifiche di incidente 01/2026 + 01/2027)
- [ACN] **Monitoraggio e supporto all'implementazione degli obblighi di base**
- [ACN] **Elaborazione e adozione del modello di categorizzazione delle attività e dei servizi (aprile 2026)**

Da metà aprile 26

Terza fase attuativa

- [Soggetti] **Categorizzazione delle attività e dei servizi**
- [ACN] **Elaborazione e adozione misure rafforzate**
- [Soggetti] **Completamento dell'implementazione obblighi di base** (termine per misure di sicurezza 10/2026 + 07/2027)
- [Soggetti] **Implementazione delle misure rafforzate**

Elenco degli obblighi

Art. 7 c.1

Dal 1° gennaio al 28 febbraio di ogni anno, registrazione/aggiornamento sulla piattaforma digitale.

Art. 7 c.4

Dal 15 aprile al 31 maggio di ogni anno, aggiornamento delle informazioni.

Art. 23

Obblighi per gli organi di amministrazione e direttivi.

Art. 24

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

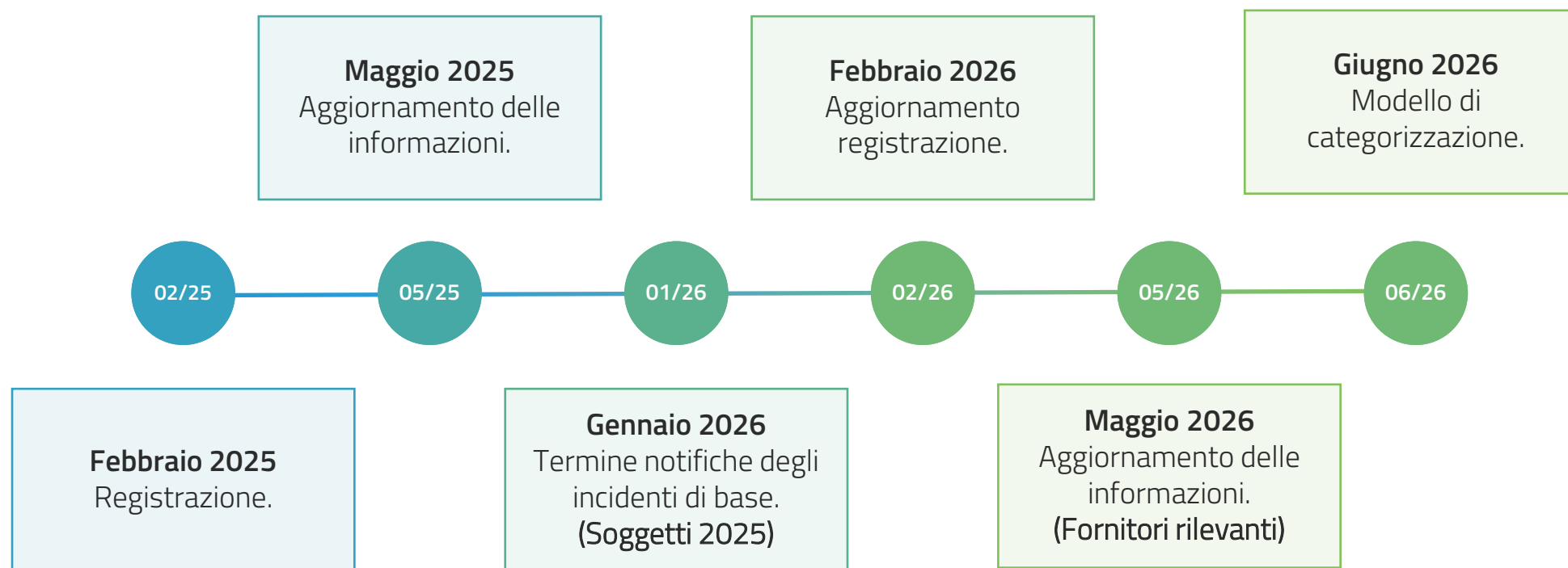
Art. 25

Obblighi in materia di notifica di incidente.

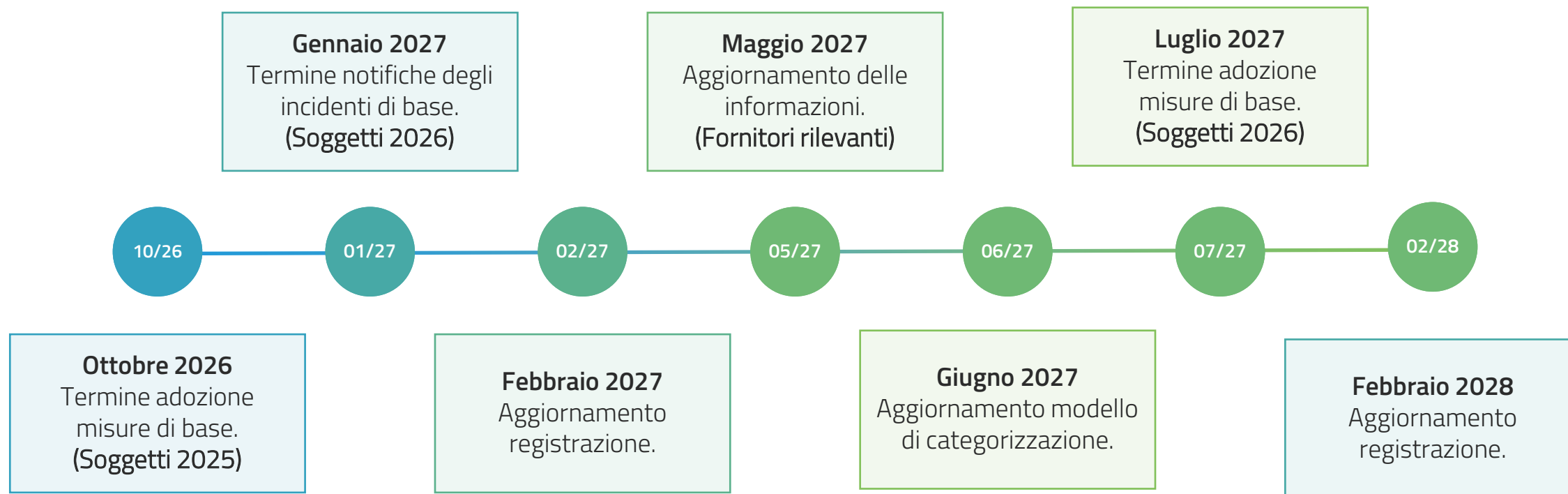
Art. 30

Dal 1° maggio al 30 giugno di ogni anno, elencazione, caratterizzazione e categorizzazione delle attività e dei servizi.

Riepilogo termini decorsi



Calendario prossime scadenze



Giro di tavolo sullo stato di attuazione della disciplina NIS, con confronto sulle principali evidenze, eventuali criticità e aspetti di particolare interesse

Quarto punto all'ordine del giorno

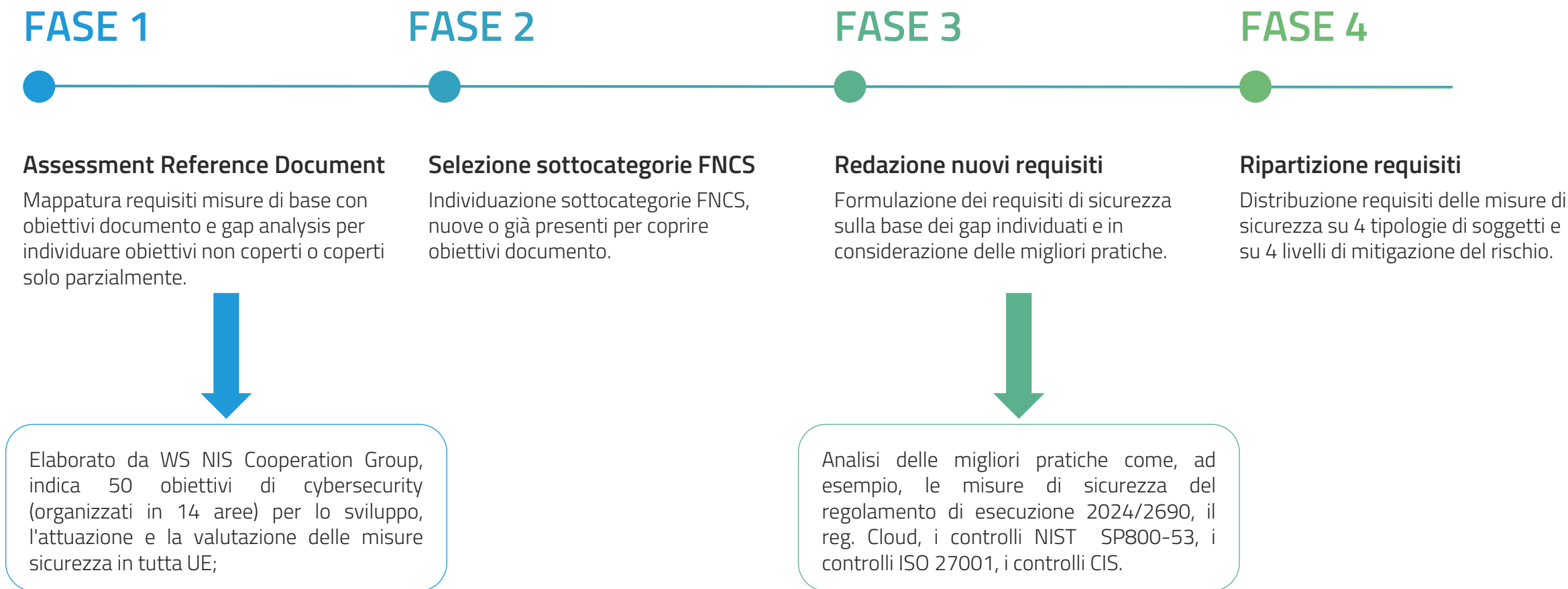


Presentazione delle misure di sicurezza rafforzate e delle relative modalità di raccolta dei riscontri.

Quinto punto all'ordine del giorno



Processo elaborazione misure rafforzate



Ripartizione requisiti su tipologie di soggetti

In accordo a quanto previsto dall'articolo 31 del decreto NIS, le *misure di base* sono state differenziate a seconda che il soggetto sia importante o essenziale. Per le *misure rafforzate* è stata considerata inoltre l'appartenenza del soggetto a 2 gruppi (A e B) individuati sulla base degli allegati del decreto NIS.

Gruppo A

- **Allegato I**
 - Energia; Spazio; Trasporti; Bancario; Infrastrutture dei mercati finanziari; Sanitario; Acqua Potabile; Acque reflue; Infrastrutture digitali; Gestione dei servizi TIC.
- **Allegato III, lettere a) e d)**
 - a) amministrazioni centrali, d) altri soggetti pubblici.
- **Allegato IV, punto 4**
 - 4. Società in house, partecipate e a controllo pubblico.

Gruppo B

- **Allegato II**
 - Servizi postali e di corriere, Gestione dei rifiuti; Fabbricazione, produzione e distribuzione sostanze chimiche; Produzione, trasformazione e distribuzione alimenti; Fabbricazione; Fornitori di servizi digitali; Ricerca.
- **Allegato III, lettere b) e c)**
 - b) amministrazioni regionali; c) amministrazioni locali.
- **Allegato IV, punti 1, 2 e 3**
 - 1. Soggetti che forniscono servizi di TPL; 2. Istituti di istruzione che svolgono attività di ricerca, 3. Soggetti che svolgono attività di interesse culturale.

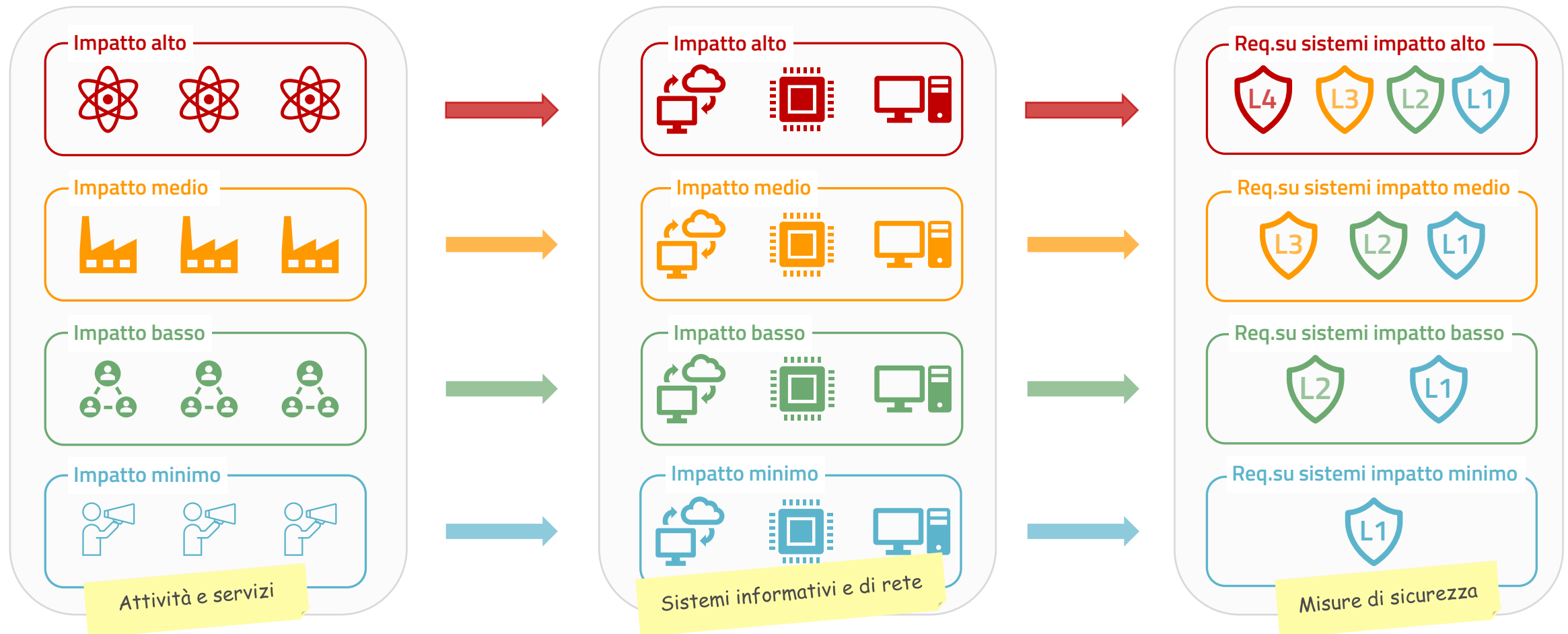
In considerazione dei due gruppi e delle distinzioni tra importanti ed essenziali, le misure rafforzate sono state differenziate sulla base dell'appartenenza del soggetto a 4 tipologie: **essenziali gruppo A, essenziali gruppo B, importanti gruppo A, importanti gruppo B.**

Misure di sicurezza rafforzate

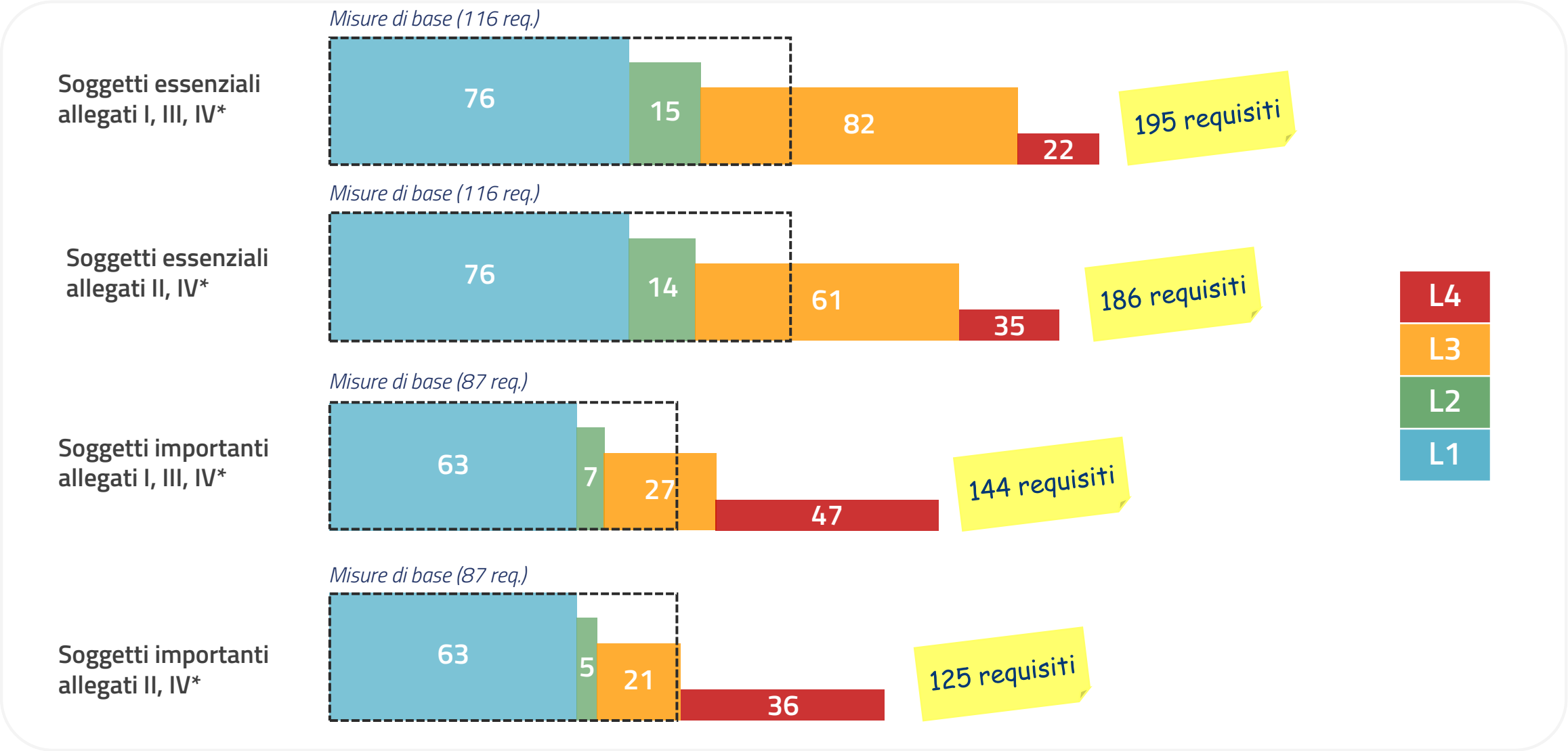
Struttura misura		
Codice	Descrizione	Requisiti
• Il codice identificativo e la descrizione della misura fanno riferimento al FNCS versione 2025. • I requisiti indicano ciò che è richiesto ai fini dell'implementazione.		
Misure di sicurezza		Requisiti
• 52 (37) per soggetti importanti gruppo B. • 52 (37) per soggetti importanti gruppo A. • 61 (43) per soggetti essenziali gruppo B. • 62 (43) per soggetti essenziali gruppo A.		• 125 (87) per soggetti importanti gruppo B. • 144 (87) per soggetti importanti gruppo A. • 186 (116) per soggetti essenziali gruppo B. • 195 (116) per soggetti essenziali gruppo A.

Ripartizione requisiti su livelli di mitigazione del rischio

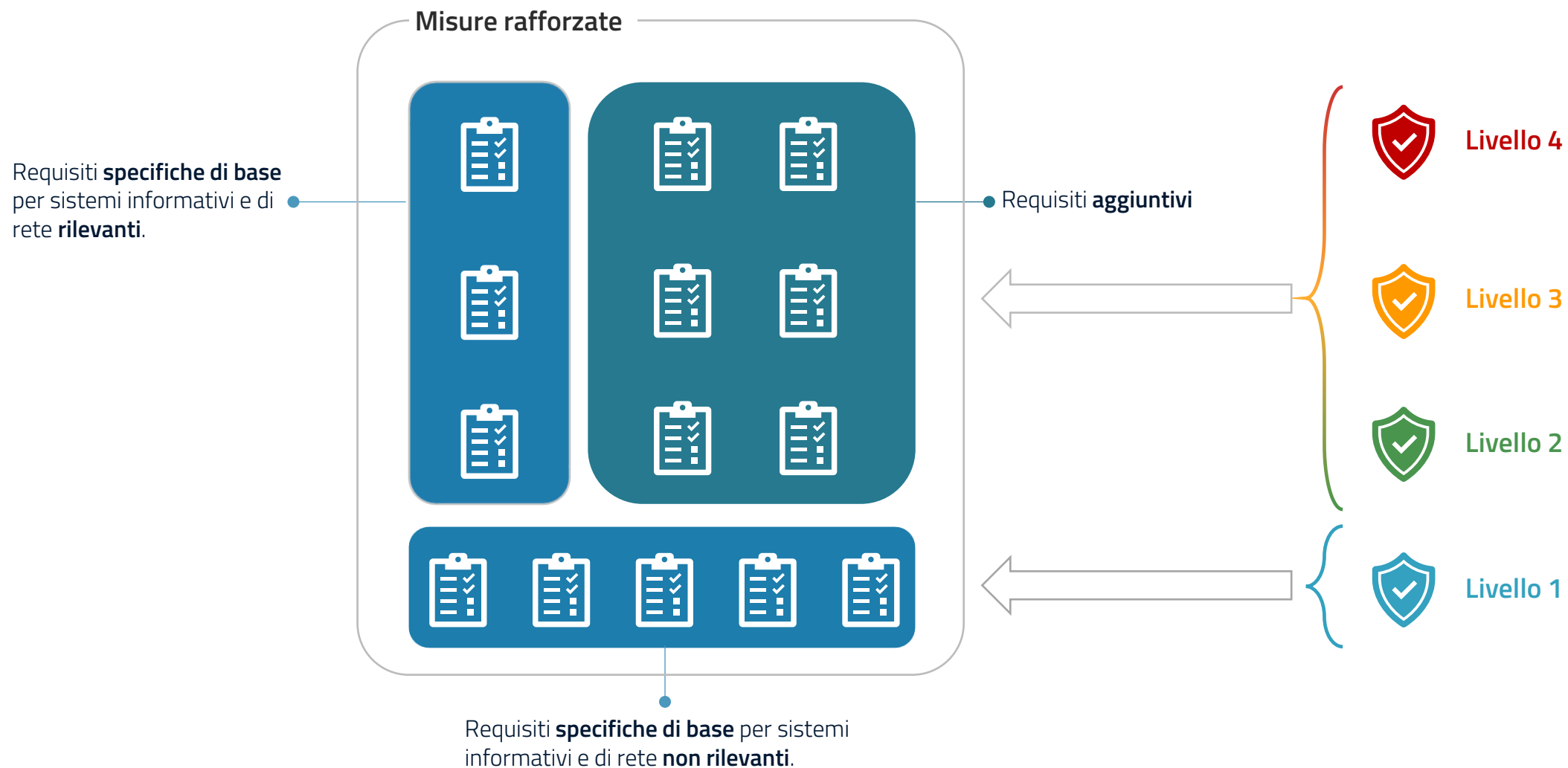
- Le misure sono differenziate sulla base delle categorie di rilevanza di attività e dei servizi che i sistemi informativi e di rete supportano, svolgono o erogano.
- Le misure di sicurezza rafforzate sono state articolate assegnando a ciascun requisito un **livelli di mitigazione del rischio** ricompreso tra L1, L2, L3 e L4.
- Il livello di mitigazione individua i sistemi sui quali il requisito deve essere implementato, in funzione della corrispondenza tra livello e categorie di rilevanza.



Ripartizione requisiti per tipologie di soggetto



Requisiti misure rafforzate e di base



Esempio misura di sicurezza

PR.DS-01 ← Codice identificativo

La riservatezza, l'integrità e la disponibilità dei dati a riposo (data-at-rest) sono protette. ← Descrizione

Requisiti

PUNTO	REQUISITO	E_A	E_B	I_A	I_B
1	Fatte salve motivate e documentate ragioni normative o tecniche, è disabilitata l'auto esecuzione dei supporti rimovibili ed è effettuata la loro scansione al fine di rilevare codici malevoli prima che siano utilizzati nei sistemi informativi e di rete.	L1	L1	L1	L1
2	Per almeno i sistemi informativi e di rete significativi, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, i dati memorizzati sui dispositivi portatili, ivi inclusi laptop, smartphone e tablet, e sui supporti rimovibili, sono cifrati con protocolli e algoritmi allo stato dell'arte e considerati sicuri.	L3	L3	L4	L4
3	Per almeno i sistemi informativi e di rete significativi, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, i dati presenti su dispositivi atti alla memorizzazione sono cancellati in modo sicuro prima della dismissione di tali dispositivi, ovvero i medesimi dispositivi sono distrutti ove necessario.	L4	L4	//	//
4	Per almeno i sistemi informativi e di rete significativi, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, sono cifrati con protocolli e algoritmi allo stato dell'arte e considerati sicuri anche i dati memorizzati sui sistemi informativi e di rete non ricompresi in quelli indicati al punto 2.	L4	//	//	//

- Requisiti di base per sistemi non rilevanti
- Requisiti di base per sistemi rilevanti
- Nuovi requisiti

E_A	Soggetti essenziali allegati I, III lett. a) e d), IV punto 4.
E_B	Soggetti essenziali allegati II, III lett. b) e c), IV punti 1, 2 e 3.
I_A	Soggetti importanti allegato I, III lett. a) e d), IV punto 4.
I_B	Soggetti importanti allegati II, III lett. b) e c), IV punti 1, 2 e 3.

Approccio basato sul rischio – Clausole requisiti

Per almeno i sistemi informativi e di rete significativi

Il soggetto ha la facoltà di limitare l'ambito di applicazione ai soli sistemi informativi di rete **significativi**.

In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05

Le modalità di attuazione (**come** è applicato il requisito) e l'ambito di attuazione (**dove** è applicato il requisito) sono definiti in funzione dei risultati della valutazione del rischio fatta dal soggetto ai sensi della misura ID.RA-05.

Fatte salve motivate e documentate ragioni normative o tecniche

Il soggetto può derogare dall'applicazione se sussistono vincoli normativi (ad esempio, leggi o regolamenti) o tecnici (ad esempio, limiti tecnologici o funzionali) che non ne permettano l'implementazione.

Forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete

Il soggetto ha la facoltà di limitare l'ambito di attuazione delle relative disposizioni alle forniture la cui eventuale compromissione può determinare effetti sulla sicurezza dei sistemi informativi e di rete.

Clausola	E_A	E_B	I_A	I_B
<i>Per almeno i sistemi informativi e di rete significativi</i>	50	42	28	23
<i>In accordo agli esiti della valutazione del rischio di cui alla misura</i>	53	45	26	17
<i>Fatte salve motivate e documentate ragioni normative o tecniche</i>	48	41	26	16
<i>Forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete</i>	3	3	3	3

Nuovi requisiti che richiedono soluzioni tecnologiche

Requisito	Descrizione	E_A	E_B	I_A	I_B
PR.AA-03.3	In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato sistemi di autenticazione, autorizzazione e registrazione centralizzati degli accessi (come, ad esempio, lo IAM).	L3	L3	L4	//
PR.AA-03.5	Per almeno i sistemi informativi e di rete significativi, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato sistemi per la gestione delle utenze con privilegi amministrativi (come, ad esempio, il PAM).	L4	L4	//	//
PR.DS-10.1	In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono presenti, aggiornati, mantenuti e configurati in modo adeguato sistemi per proteggere i sistemi informativi e di rete dagli attacchi di tipo denial of service , o comunque a limitarne gli impatti.	L3	L3	L4	//
PR.IR-01.10	In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono presenti, aggiornati, mantenuti e configurati in modo adeguato firewall sui punti terminali (host-based firewall).	L3	L3	L4	L4
PR.IR-01.12	L'accesso remoto ai sistemi di amministrazione è effettuato tramite rete privata virtuale (VPN) o soluzioni equivalenti in termini di sicurezza informatica.	L3	L3	L4	L4
PR.IR-01.13	In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, l'accesso remoto ai sistemi informativi e di rete interni è effettuato tramite rete privata virtuale (VPN) o soluzioni equivalenti in termini di sicurezza informatica.	L3	L3	L4	//
PR.IR-01.14	In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono presenti, aggiornati, mantenuti e configurati in modo adeguato sistemi di prevenzione delle intrusioni (come, ad esempio, IPS).	L4	L4	//	//
DE.CM-01.5	In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono presenti, aggiornati, mantenuti e configurati in modo adeguato sistemi di rilevamento delle intrusioni (come, ad esempio, IDS).	L3	L4	//	//
DE.CM-09.3	Per almeno i sistemi informativi e di rete significativi, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono presenti, aggiornati, mantenuti e configurati in modo adeguato strumenti tecnici di analisi e filtraggio del traffico in uscita (ivi inclusa la navigazione Internet).	L3	L3	L4	//
DE.CM-09.4	Fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato, sistemi di rilevamento e risposta sui punti terminali (come, ad esempio, EDR).	L3	L3	L4	//
DE.CM-09.7	Ai fini rilevamento del codice malevolo, fatte salve motivate e documentate ragioni normative o tecniche, i sistemi di protezione dei punti terminali (endpoint) di cui al punto 1 rilevano il codice malevolo anche sulla base del comportamento (behavior based).	L4	//	//	//
DE.AE-03.1	Sono presenti, aggiornati, mantenuti e configurati in modo adeguato sistemi per la gestione delle informazioni e degli eventi di sicurezza (come, ad esempio, il SIEM) per (...):	L3	L4	//	//



Tempistiche di adozione

Tempistiche adozione misure a regime

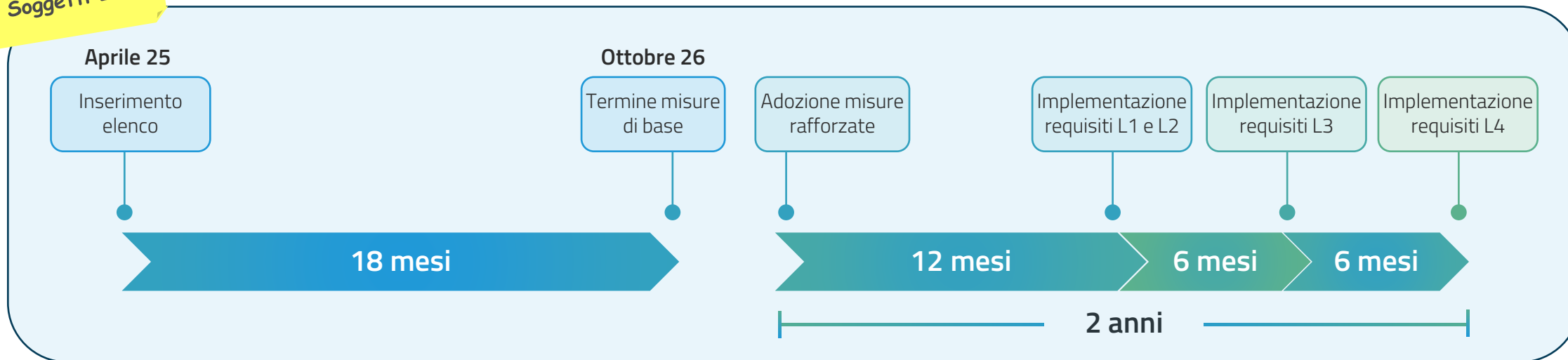
In definizione



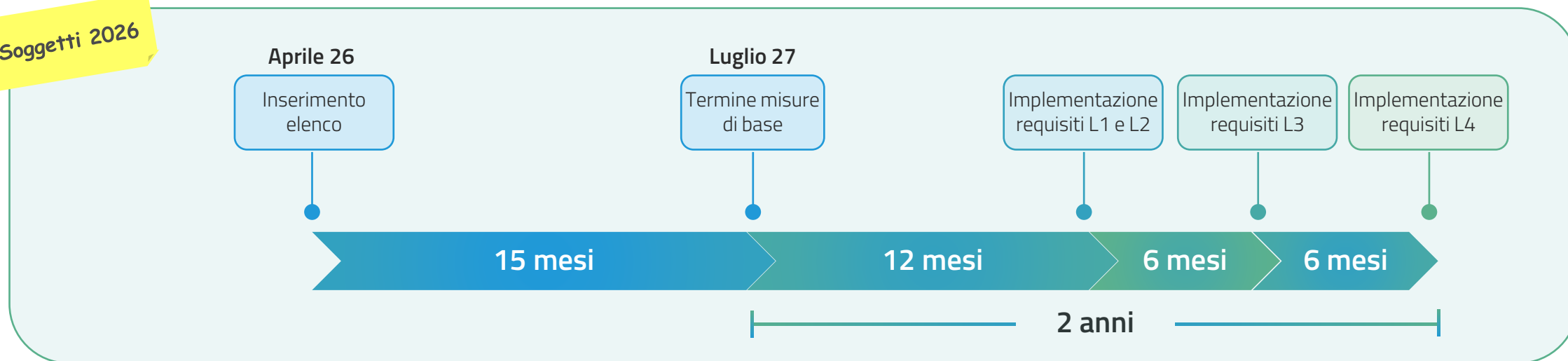
Tempistiche adozione misure per soggetti 2025, 2026

In definizione

Soggetti 2025



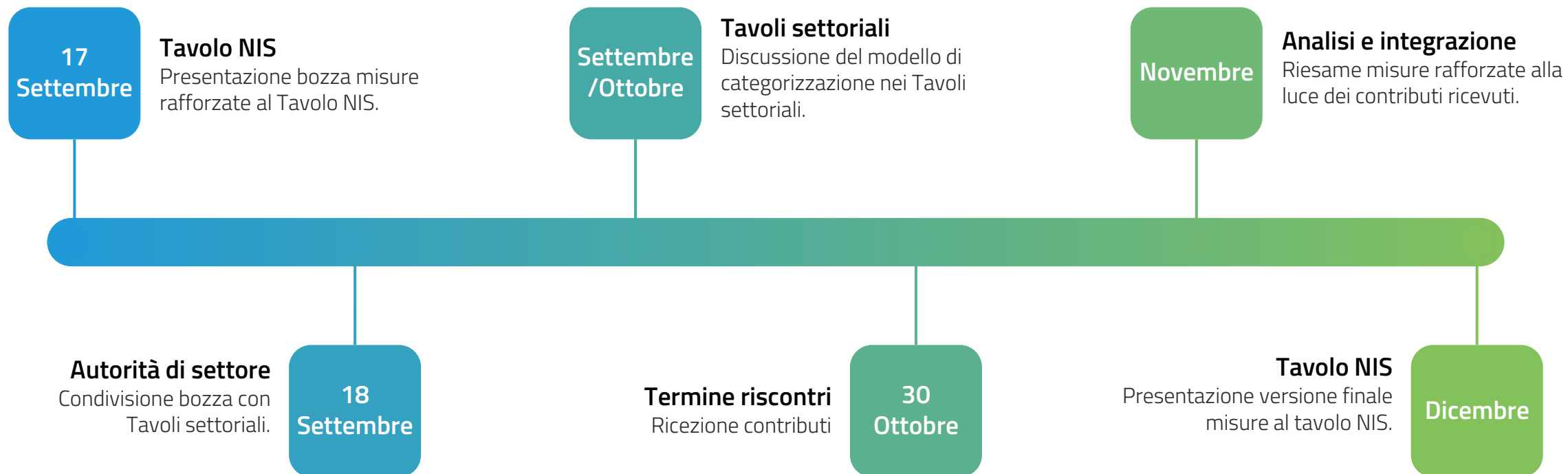
Soggetti 2026





Processo di adozione

Processo adozione misure rafforzate



Materiale di supporto: modulo Excel per revisione misure

Distribuzione dei moduli

- File Excel distinto tra soggetti gruppo A e B.
- Ogni autorità riceve i file relativi alle tipologie di soggetto di propria competenza.

Struttura modulo

- **Commenti generali:** osservazioni di carattere generale.
- **Commenti su requisiti:** commenti sui singoli requisiti anche volti a modificare il relativo livello di mitigazione.
- **Proposta riformulazione requisiti:** possibilità di proporre una nuova formulazione del requisito.
- **Proposta nuove requisiti:** possibilità di proporre un nuovo requisito e associare il relativo livello di mitigazione.

Materiale di supporto: guida alla lettura misure rafforzate



INDICE	
1. Introduzione	1
1.1. Premessa	1
1.2. Scopo e organizzazione del documento	2
1.3. Ambito di applicazione	2
1.4. Termini e definizioni	2
1.5. Norme di riferimento	3
2. Misure di sicurezza rafforzate	4
2.1. Quadro generale	4
2.2. Livelli di mitigazione del rischio	7
2.3. Assegnazione del livello di mitigazione ai requisiti di base	8
Appendice A – File Excel per la revisione delle misure	9
Appendice B – Processo di elaborazione delle misure	10
Appendice C – Clausole requisiti misure di sicurezza	12
Appendice D – Requisiti misure con clausole	15

Linee Guida NIS – Misure di sicurezza rafforzate | Guida alla lettura.

Giro di tavolo e confronto sulle misure di sicurezza rafforzate, prime impressioni ed eventuali elementi di interesse emersi

Sesto punto all'ordine del giorno



Chiusura dei lavori.

Settimo punto all'ordine del giorno



<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/>

