Clusit

SECURITY SUMMIT

ASTREA

NIS2, dalle misure di base alla categorizzazione: guida ai prossimi passi del percorso di adeguamento.

29 aprile 2026

9.20 Apertura e moderazione dei lavori a cura di **Luca Bechelli**, CD CLUSIT

9.30 Intervento a cura di: **Milena Antonella Rizzi**, Capo Servizio Regolazione dell'**Agenzia per la Cybersicurezza Nazionale**

Interviene: **Claudio Telmon**, CD Clusit

11.00 Q&A

12.00 Conclusioni a cura di **Anna Vaccarelli**, Presidente CLUSIT

12.15 Cocktail

Clusit

SECURITY SUMMIT

ASTREA

NIS2, dalle misure di base alla categorizzazione: guida ai prossimi passi del percorso di adeguamento.

29 aprile 2026

9.20 Apertura e moderazione dei lavori a cura di **Luca Bechelli**, CD CLUSIT

9.30 Intervento a cura di: **Milena Antonella Rizzi**, Capo Servizio Regolazione dell'**Agenzia per la Cybersicurezza Nazionale**

Interviene: **Claudio Telmon**, CD Clusit

11.00 Q&A

12.00 Conclusioni a cura di **Anna Vaccarelli**, Presidente CLUSIT

12.15 Cocktail

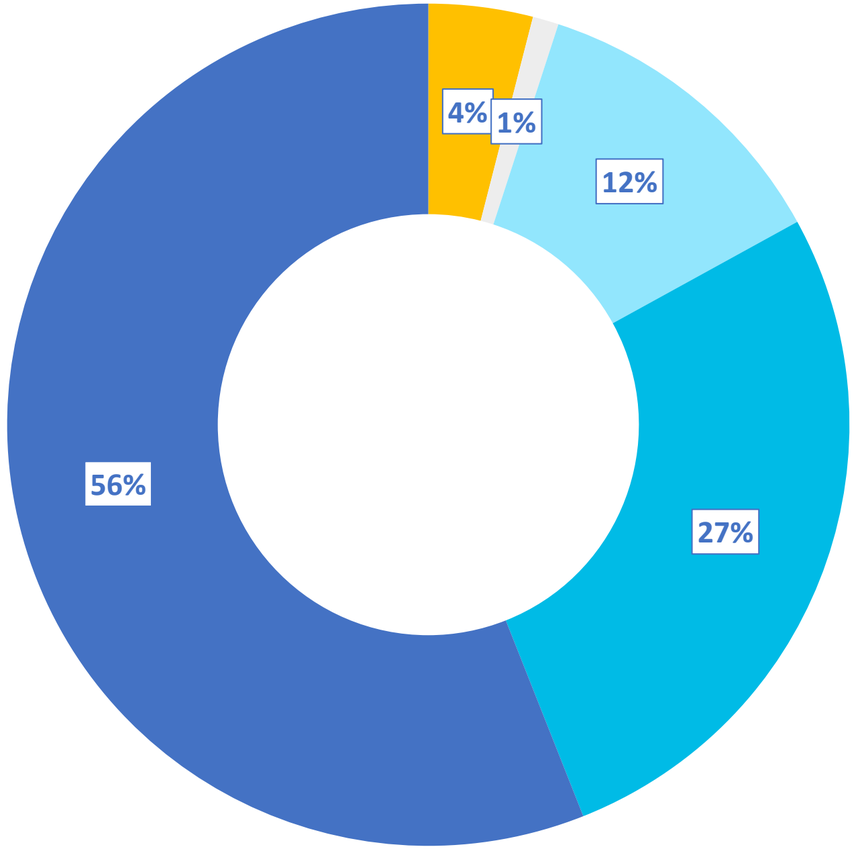
Survey CLUSIT – Politecnico di Milano

in collaborazione con l'Osservatorio
Osservatorio Cybersecurity & Data Protection

Questionario in forma anomima, on line per 2 mesi

Confronto con ACN

*Quanto **avete ritenuto utili le occasioni di confronto** organizzate con l'Agenzia per la Cybersicurezza Nazionale?*



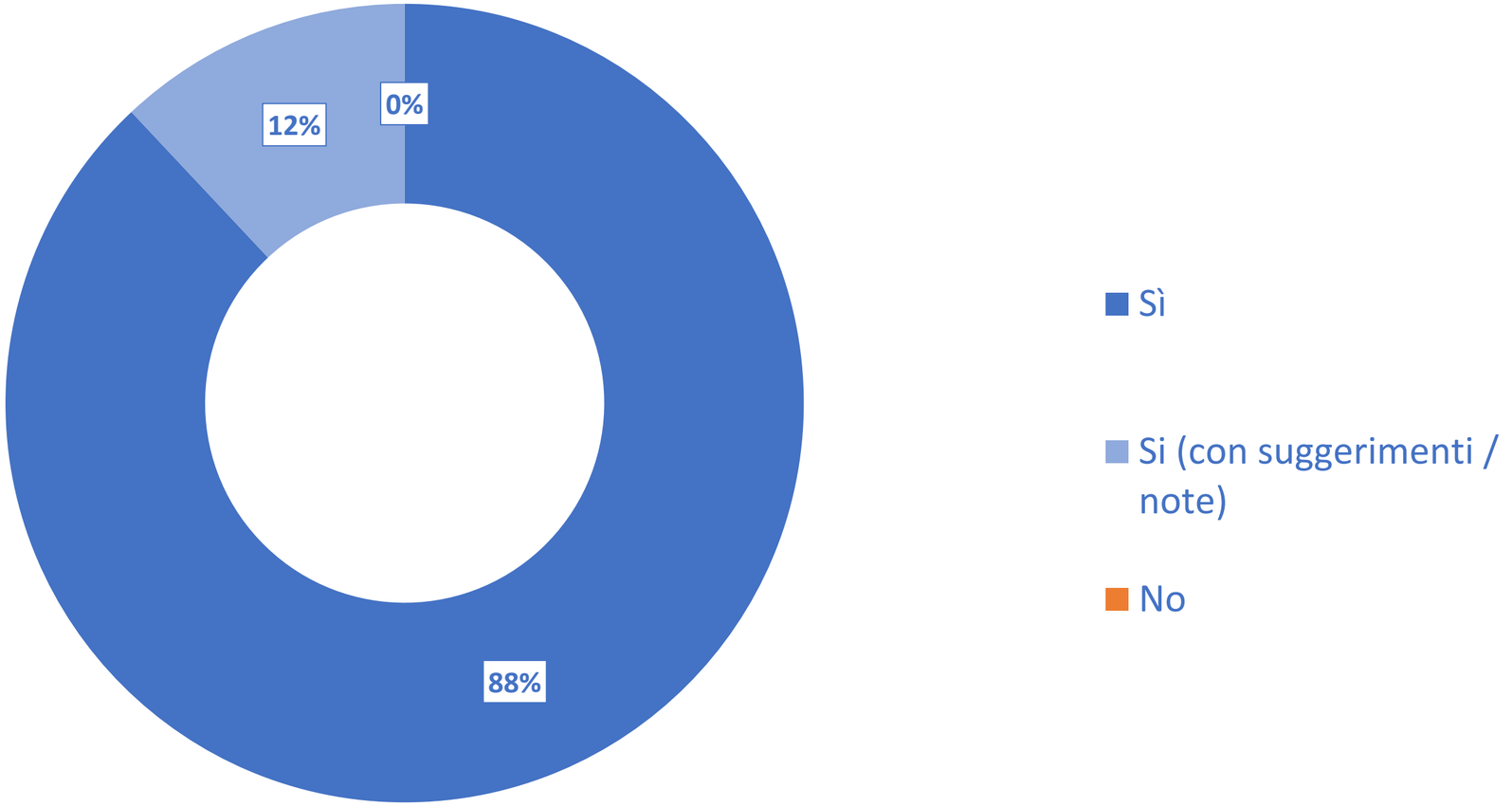
1 2 3 4 5

MINIMO MASSIMO

Campione Soggetti NIS2: 188 rispondenti anonimi

Confronto con ACN

*Riterreste utile che ne **venissero organizzate altre** durante il 2026?*



Campione Soggetti NIS2: 188 rispondenti anonimi

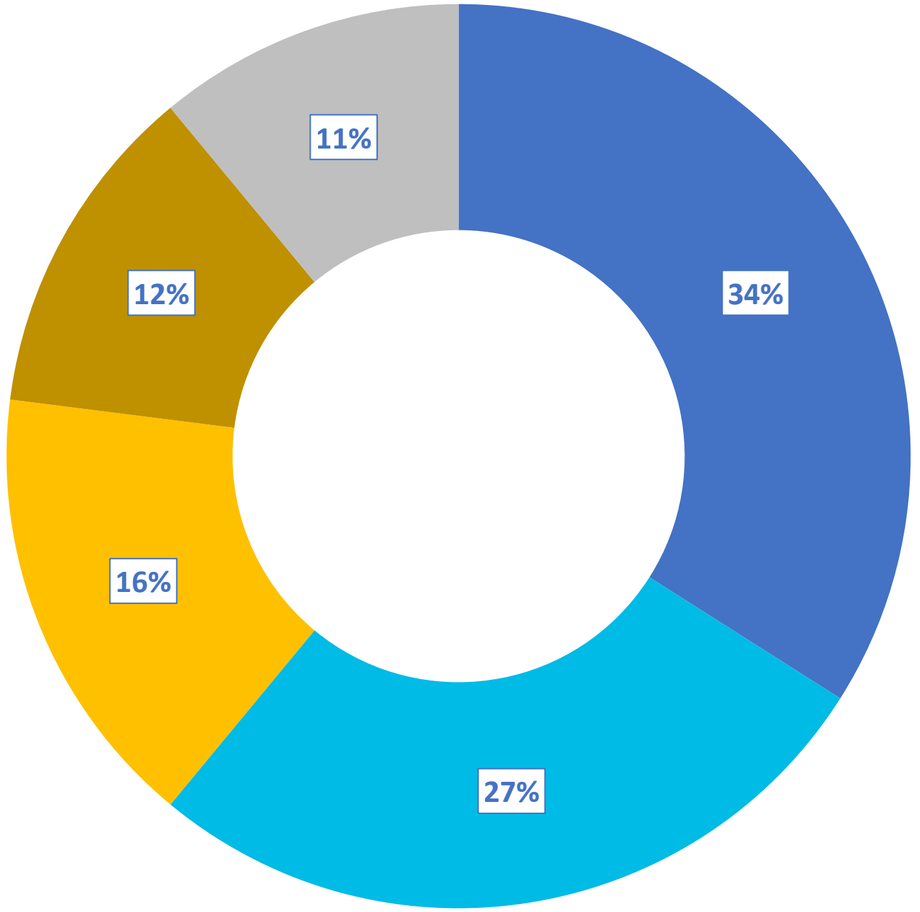
Le sfide nel percorso di adeguamento

*Quali fasi del percorso di adeguamento risultano/sono risultate/prevedete **più complesse** nella vostra organizzazione?*

Campione Soggetti NIS2: 185 rispondenti anonimi

Il ruolo degli Organi Amministrativi e Direttivi

*In riferimento alla **Responsabilizzazione degli organi Amministrativi e Direttivi** ed ai compiti ad essi attribuiti definiti nell'ambito delle misure di base, in quale affermazione, vi riconoscete maggiormente:*



- Finalmente una normativa che responsabilizza in modo chiaro e concreto i vertici della mia organizzazione sui temi della sicurezza delle informazioni
- Molto utile, ma le funzioni specialistiche in materia di IT, OT e Sicurezza delle informazioni non sempre sono preparate a relazionarsi adeguatamente con il CdA e il Top Management per supportare le decisioni in materia di cybersecurity
- Potrebbe essere utile in prospettiva, ma le modalità definite sono scarsamente utili o efficaci a perseguire l'obiettivo
- Sono adempimenti burocratici e meramente formali, hanno creato difficoltà con minimo valore aggiunto nella mia organizzazione
- Non saprei dare oggi un giudizio

Campione Soggetti NIS2: 183 rispondenti anonimi

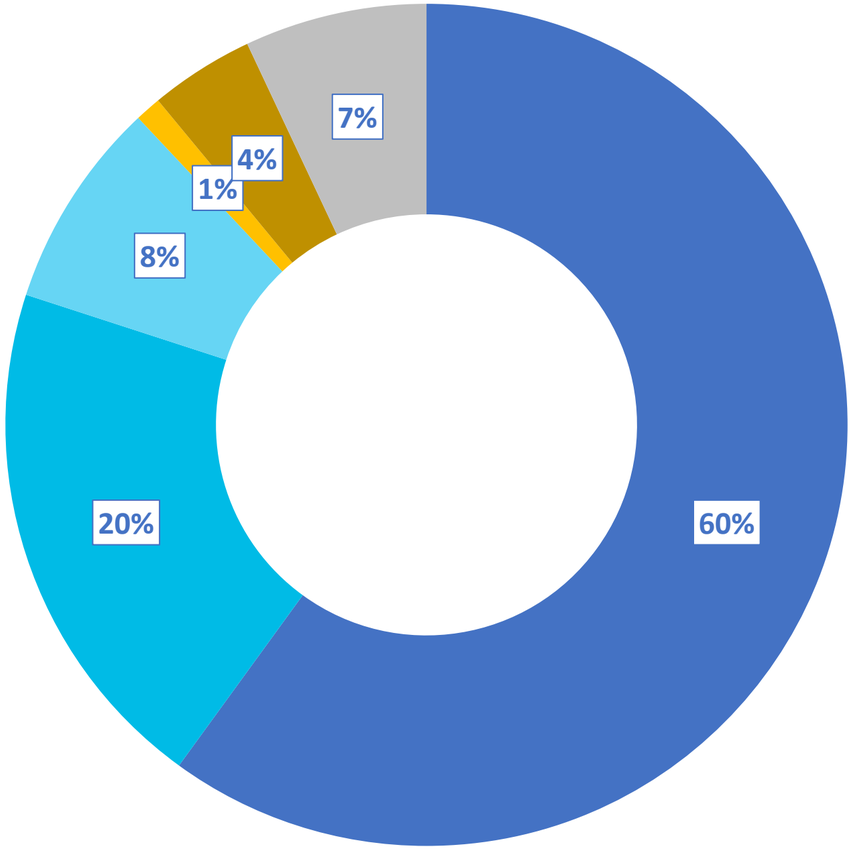
Obblighi di notifica al CSIRT

*Quali sono **gli aspetti che ritenete più critici** nell'adempimento degli obblighi di notifica verso il CSIRT Italia?*

Campione Soggetti NIS2: 186 rispondenti anonimi

Impatto della NIS2 sulla supply chain

*Ritenete che, a tendere, il fatto che nella vostra catena di fornitura **siano presenti soggetti NIS2** che hanno soddisfatto gli adempimenti previsti dalla normativa, costituisca un beneficio per la sicurezza della vostra organizzazione?*

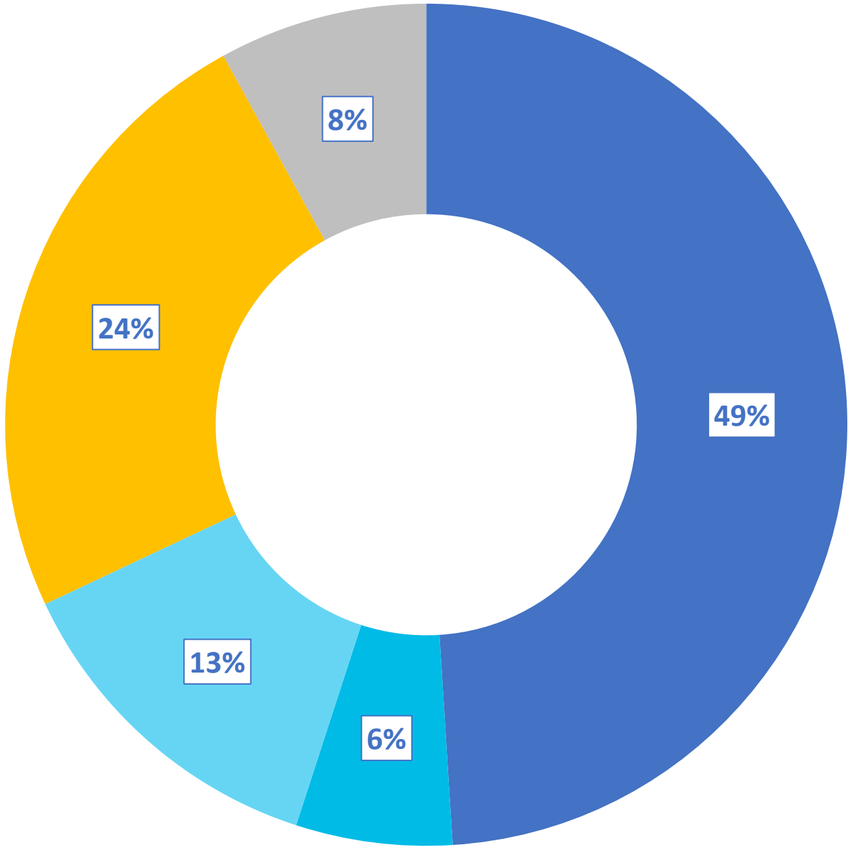


- Sì, in quanto cliente ho intenzione di inserire questa verifica nell'ambito delle mie procedure di acquisto di servizi rilevanti dal punto di vista della cybersecurity
- Sì, in quanto fornitore verso terzi, userò questa leva come vantaggio competitivo
- Sì, ma come cliente non saprei come adeguare i miei processi di acquisto per trarne reale beneficio
- No, ritengo che l'approccio alla gestione della cybersecurity dovrebbe essere lasciato alle aziende e la normativa costituisca un onere e non un vantaggio
- No, ritengo che l'appartenenza al perimetro NIS2 non costituisca di per sé un elemento di valore aggiunto
- Non saprei

Campione Soggetti NIS2: 184 rispondenti anonimi

Impatto sui fornitori di soggetti NIS

In quanto fornitore di Soggetti NIS2, le esigenze di adeguamento dei vostri clienti hanno previsto/ prevedranno delle azioni di rafforzamento della postura di sicurezza della vostra organizzazione?



Campione Fornitori (Non Soggetti NIS2): 84 rispondenti anonimi

Clusit

SECURITY SUMMIT

ASTREA

NIS2, dalle misure di base alla categorizzazione: guida ai prossimi passi del percorso di adeguamento.

29 aprile 2026

9.20 Apertura e moderazione dei lavori a cura di **Luca Bechelli**, CD CLUSIT

9.30 Intervento a cura di: **Milena Antonella Rizzi**, Capo Servizio Regolazione dell'**Agenzia per la Cybersicurezza Nazionale**

Interviene: **Claudio Telmon**, CD Clusit

11.00 Q&A

12.00 Conclusioni a cura di **Anna Vaccarelli**, Presidente CLUSIT

12.15 Cocktail

NIS2. Proporzionalità e gradualità
Specifiche di base e categorizzazione

29 aprile 2026

Fasi attuative

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 delle informazioni (termine 07/2025)
- [Soggetti] Implementazione obblighi di base (termine per notifiche di incidente 01/2026)
- [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)
- [ACN] Elaborazione obblighi a lungo termine

Da metà aprile 26

Terza fase attuativa

- [Soggetti] Aggiornamento annuale delle informazioni (indicazione fornitori rilevanti)
- [Soggetti] Categorizzazione delle attività e dei servizi
- [Soggetti] Completamento dell'implementazione obblighi di base (termine per misure di sicurezza 10/2026)
- [ACN] Elaborazione e adozione obblighi a lungo termine
- [Soggetti] Implementazione degli obblighi a lungo termine

Registrazione 2026 – Esiti

Oltre 30K organizzazioni censite

Oltre 20K soggetti NIS

Oltre 5K soggetti essenziali

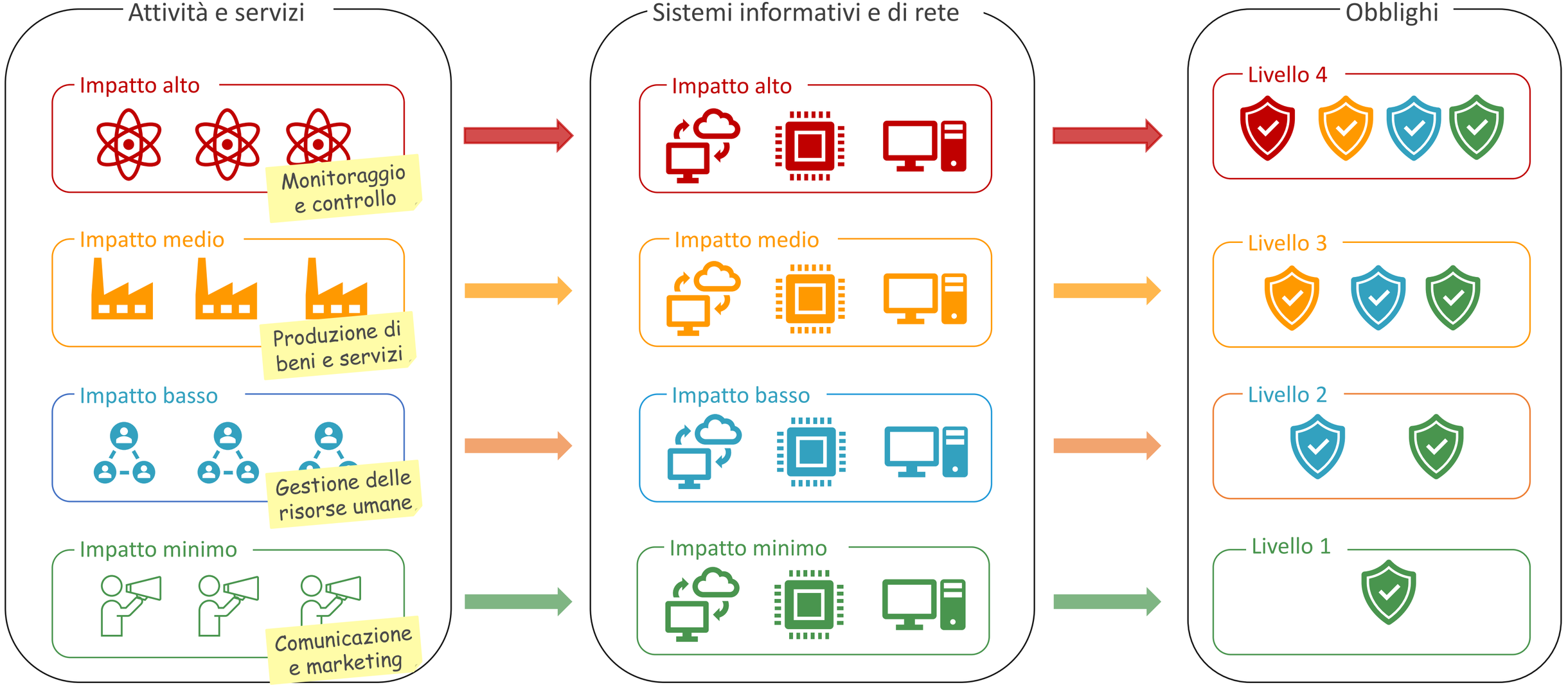
Comunicazioni trasmesse il 13 e 14 aprile

L’elenco dei soggetti NIS è escluso dall’accesso agli atti

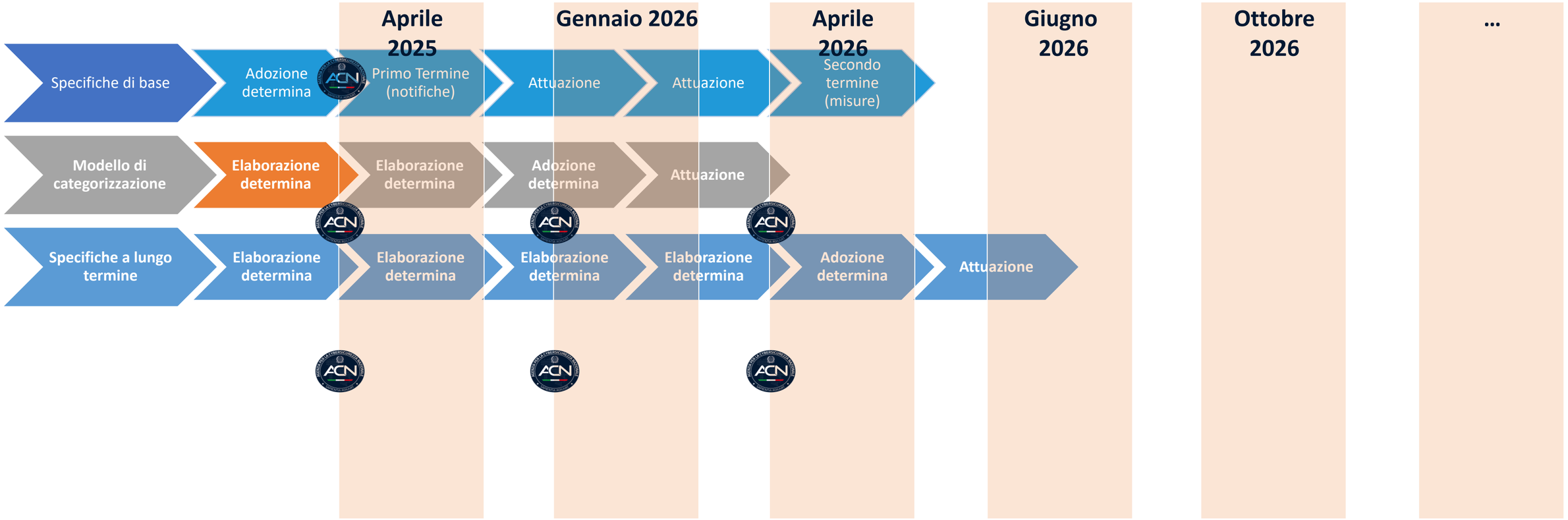
Proporzionalità e gradualità

Proporzionalità degli obblighi

Esempio su 4 livelli



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.

Specifiche di base

Modello concettuale specifiche di base

Attività e servizi

Attività e servizi NIS

Usufruiscono di

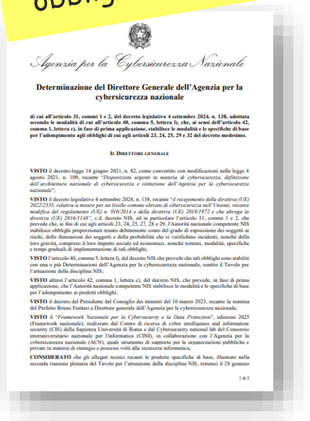
Utenti e clienti

La loro compromissione comporterebbe un impatto significativo su R, I, D attività e servizi ambito decreto NIS.

Sono erogati tramite

Gli allegati tecnici costituiscono le specifiche di base

Determina ACN obblighi di base


Agenzia per la Cybersicurezza Nazionale

Determinazione del Direttore Generale dell'Agenzia per la cybersicurezza nazionale

di cui all'articolo 31, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo.

IL DIRETTORE GENERALE

Misure di sicurezza

Si applicano a

Incidenti

Occorrono su

Sistemi informativi e di rete

Sistemi informativi e di rete rilevanti

Misure di sicurezza di base

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

- 37 per soggetti importanti ed essenziali.
- 6 per i soli soggetti essenziali.

Requisiti

- 87 per soggetti importanti ed essenziali.
- 29 per i soli soggetti essenziali.

Struttura misure di sicurezza

PR.DS-11 ← Codice identificativo

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

Requisiti

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

Specifiche di base (notifiche di incidente)

Incidenti significativi di base

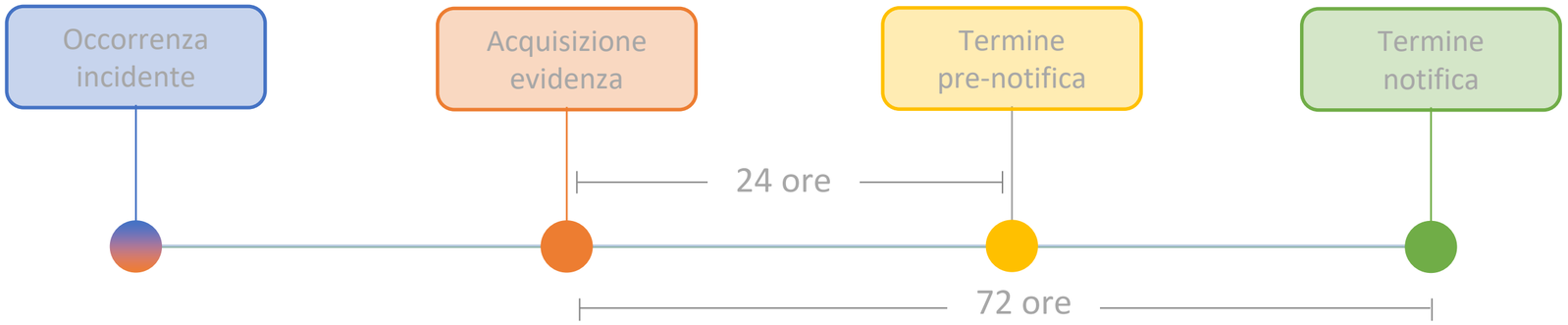
IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita 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

Solo soggetti essenziali

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.



Modello di categorizzazione

Base giuridica

Art. 30

Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi

1. Ai fini di cui all'articolo 24, comma 1, dal 1° maggio al 30 giugno di ogni anno a partire dalla ricezione della prima comunicazione di cui all'articolo 7, comma 3, lettera a), i soggetti essenziali e i soggetti importanti comunicano e aggiornano, tramite la piattaforma digitale di cui all'articolo 7, comma 1, un elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro caratterizzazione e della relativa attribuzione di una categoria di rilevanza.

2. L'Autorità nazionale competente NIS stabilisce, secondo le modalità di cui all'articolo 40, comma 5, anche tenuto conto di quanto previsto dall'articolo 25, comma 1, le categorie di rilevanza nonché il processo, le modalità e i criteri per l'elencazione, caratterizzazione e categorizzazione delle attività e dei servizi di cui al presente articolo.

3. Entro novanta giorni dalla comunicazione tramite la piattaforma digitale di cui al comma 1, l'Autorità nazionale competente NIS fornisce riscontro ai soggetti essenziali e ai soggetti importanti circa la conformità di quanto comunicato rispetto alle modalità e ai criteri di cui al comma 2. Il predetto termine può essere prorogato dall'Autorità nazionale competente NIS, per una sola volta e fino ad un massimo di ulteriori sessanta giorni, qualora sia necessario svolgere approfondimenti. Ove si renda necessario richiedere integrazioni e informazioni aggiuntive ai soggetti essenziali o importanti, i termini di cui al presente comma sono interrotti sino alla data di ricevimento delle predette integrazioni e informazioni, che sono rese entro il termine di trenta giorni dalla richiesta.

4. In assenza del riscontro di cui al comma 3 da parte dall'Autorità nazionale competente NIS entro i termini di cui al medesimo comma, la conformità di cui al comma 3 si intende convalidata.

5. Ai fini del presente articolo, l'Autorità nazionale competente NIS può avvalersi dei tavoli settoriali di cui all'articolo 11, comma 4, lettera f).

Modello di categorizzazione

Elenco attività e servizi

- Norma la predisposizione e la compilazione dell'elenco delle attività e dei servizi dei soggetti NIS.

Categorie di rilevanza

- Definisce le categorie di rilevanza delle attività e dei servizi dei soggetti NIS e le modalità di attribuzione delle stesse.

Modello semplificato per soggetti PA

- Riutilizza gli esisti della classificazione di dati e servizi prevista dal Regolamento Cloud.

Modello di categorizzazione

Elementi del modello

- ✓ Definita una struttura delle attività e i servizi organizzata in 10 macro-aree ognuna caratterizzata da denominazione, descrizione, elenco di esempi, categoria di rilevanza preassegnata.
- ✓ Ogni macro-area rappresenta un insieme astratto di attività e servizi di un'organizzazione caratterizzati da elementi in comune quali, ad esempio, utenti, finalità o tipologia di prestazione.
- ✓ Per le macro aree Produzione di beni e servizi e Monitoraggio e controllo gli esempi sono stati declinati sulla base della tipologia di soggetto (*esempi specifici*).

Categorie di rilevanza

- ✓ 4 categorie sulla base dell'impatto di una compromissione sulle capacità dell'organizzazione di erogare le attività e i servizi per i quali rientra nell'ambito dell'applicazione del decreto NIS (*attività e servizi NIS*):
  - impatto minimo
  - impatto basso
  - impatto medio
  - impatto alto

Macro-area

Ogni macro-area rappresenta un contenitore di attività e servizi ed è caratterizzata da denominazione, descrizione, elenco di esempi (*per 2 macro-aree, gli esempi forniti sono specifici sulla base della tipologia di soggetto*) e categoria di rilevanza pre-assegnata.

Ogni soggetto inserisce proprie attività e propri servizi che rientrano nella macro area, eventualmente modificando la categoria di rilevanza a livello di singola attività o servizio. Se non dovesse avere alcuna attività o servizio, rimuove la macro-area.

Elenco macro aree

Minimo	Altri servizi e attività
Minimo	Comunicazione e marketing
Minimo	Gestione amministrativa
Minimo/ Basso	Logistica
Basso	Gestione delle risorse umane
Basso	Gestione dei clienti
Basso	Gestione finanziaria
Medio	Produzione di beni e servizi
Medio	Ricerca, sviluppo e progettazione
Alto	Monitoraggio e controllo

Processo di elencazione e categorizzazione

FASE 1

Identificazione attività/servizi

Sono individuati tutti i servizi e le attività dell'organizzazione

FASE 2

Mappatura attività/servizi in macro-aree

Le attività e i servizi individuati sono associate alle macro-aree definite dal modello di categorizzazione.

FASE 3

Attribuzione categorie di rilevanza

Per ogni attività/servizio individuato è assegnata una categoria di rilevanza.

- ✓ I soggetti visualizzano l'elenco delle 10 macro-aree comprensive di denominazione, descrizione, esempi e categoria di rilevanza pre-assegnata;
- ✓ I soggetti inseriscono le proprie attività e i propri servizi corrispondenti alle macro-aree visualizzate;
- ✓ Qualora non sia inserita alcuna attività/servizio in una macro-area, quella macro-area non sarà considerata ai fini dell'elencazione.
- ✓ Le attività e i servizi inseriti acquisiscono, per impostazione predefinita, la categoria di rilevanza della macro-area corrispondente.
- ✓ I soggetti potranno modificare, motivando adeguatamente, la categoria di rilevanza sia a livello di macro-area che di singolo attività/servizio.
- ✓ Qualora un soggetto ritenesse che un'attività/servizio non rientri in alcuna delle macro-aree individuate, potrà utilizzare la macro-area denominata *Altri servizi e attività*.

Coordinamento con classificazione dati e servizi per PA

Modello semplificato

- ✓ Art. 3 del Decreto Direttoriale ACN n. 21007/24 (cosiddetto Regolamento Cloud) prevede che le PA predispongano e aggiornino un elenco dei propri dati e dei propri servizi digitali.
- ✓ In considerazione di quanto previsto dal Reg. Cloud, i soggetti NIS che hanno svolto la classificazione dei dati e dei servizi (Regolamento Cloud) applicano il modello stabilito dal Regolamento Cloud ai fini dell'elencazione e categorizzazione delle attività e dei servizi, in luogo del modello di categorizzazione descritto nel precedente paragrafo.
- ✓ Per tali soggetti l'elenco delle attività e dei servizi dei soggetti delle pubbliche amministrazioni è pertanto costituito dall'elenco dei dati e servizi digitali classificati ai sensi del Regolamento Cloud e le categorie di rilevanza coincidono con le classi previste da medesimo regolamento (ordinari, critici, strategici).
- ✓ Eventuali modifiche, come ad esempio l'inserimento o rimozione di attività/servizi o la variazione della categoria di rilevanza, dovranno essere coerenti con la classificazione dei dati e servizi effettuata ai fini del *Regolamento Cloud*.

Finalità dell'elencazione e categorizzazione

Proporzionalità misure di sicurezza

- ✓ L’elencazione e categorizzazione è finalizzata ad aggregare attività e servizi in relazione alle categorie di rilevanza del modello di categorizzazione in modo da prevedere – sui relativi sistemi informativi e di rete – misure di sicurezza proporzionate a tali categorie.
- ✓ In accordo a quanto previsto dall’art. 42 del decreto (*fase di prima applicazione*) sono state definite le misure di sicurezza di base che saranno integrate da misure di sicurezza aggiuntive – con requisiti di livello avanzato rispetto a quelli delle misure di base – in modo da stabilire le cosiddette misure di sicurezza a lungo termine che riguarderanno le fasi successive a quella di prima applicazione.
- ✓ Le misure a lungo termine definiranno 4 *set* di misure di sicurezza definite su 4 livelli di mitigazione del rischio crescente (L1, L2, L3, L4) e differenziate tra soggetti essenziali e importanti:
  - per i soggetti privati, ognuna delle 4 categoria di rilevanza corrisponde a un set di misure di sicurezza;
  - per i soggetti pubblici, i sistemi informativi e di rete oggetto del regolamento cloud classificati come ordinari, critici, strategici implementano le misure di sicurezza L2, L3 e L4, i restanti sistemi informativi e di rete (infrastruttura informatica client) implementano le misure di sicurezza di livello L1.

Categoria di rilevanza e misure di sicurezza (1/2)

Proposta su 4 livelli

Sistemi informativi e di rete soggetti privati

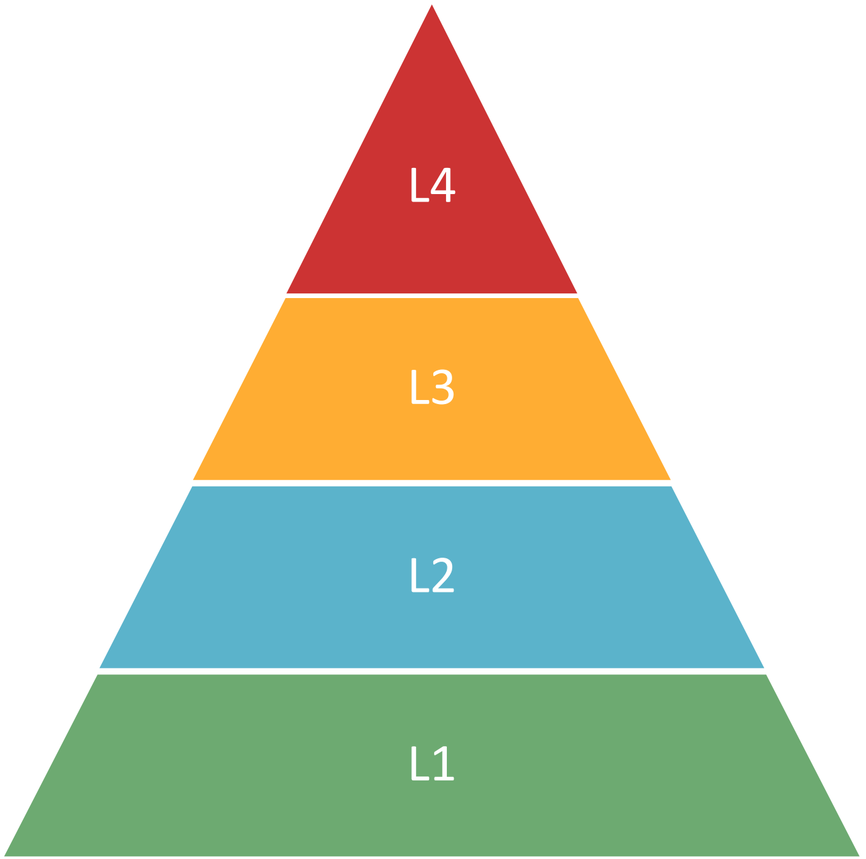
Impatto alto

Impatto medio

Impatto basso

Impatto minimo

Misure di sicurezza a lungo termine



Sistemi informativi e di rete soggetti pubblici

Reg. Cloud strategico

Reg. Cloud critico

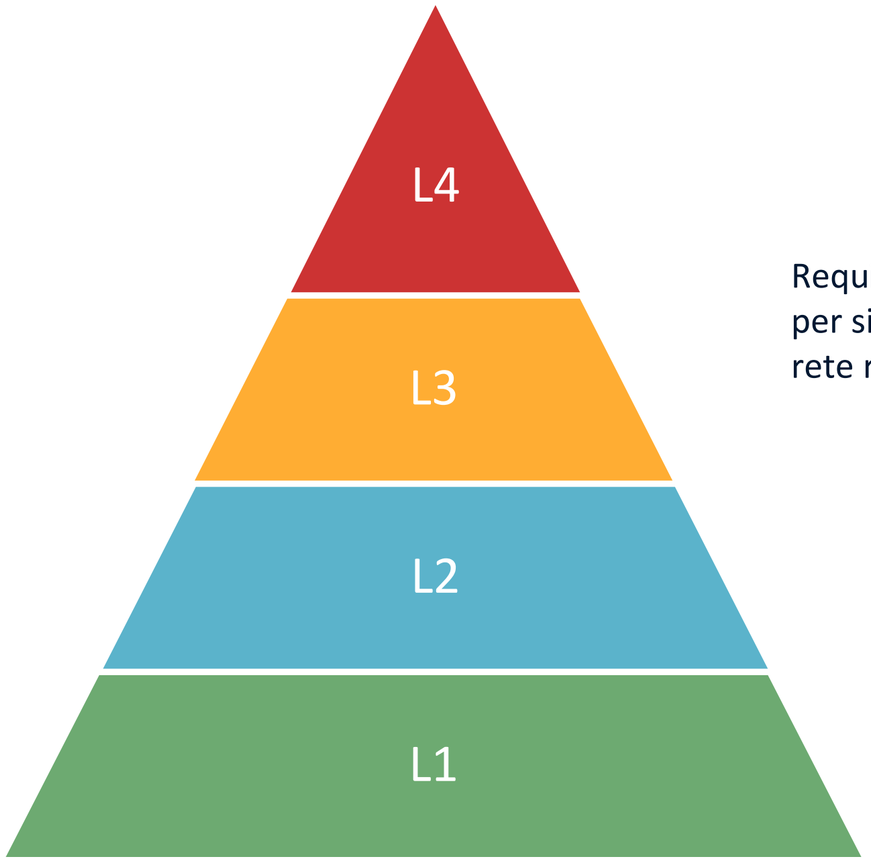
Reg. Cloud ordinario

Fuori ambito Reg. Cloud

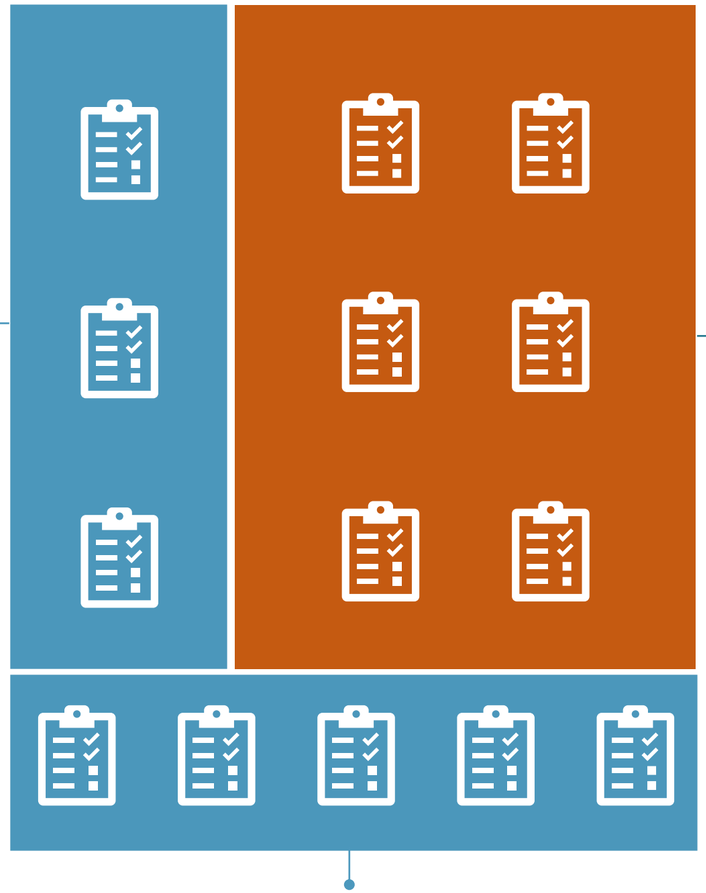
Categoria di rilevanza e misure di sicurezza (2/2)

Proposta su 4 livelli

Misure di sicurezza a lungo termine



Requisiti specifiche di base per sistemi informativi e di rete rilevanti.



Requisiti aggiuntivi

Requisiti specifiche di base per sistemi informativi e di rete non rilevanti.

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/

Clusit

SECURITY SUMMIT

ASTREA

NIS2, dalle misure di base alla categorizzazione: guida ai prossimi passi del percorso di adeguamento.

29 aprile 2026

9.20 Apertura e moderazione dei lavori a cura di **Luca Bechelli**, CD CLUSIT

9.30 Intervento a cura di: **Milena Antonella Rizzi**, Capo Servizio Regolazione dell'**Agenzia per la Cybersicurezza Nazionale**

Interviene: **Claudio Telmon**, CD Clusit

11.00 Q&A

12.00 Conclusioni a cura di **Anna Vaccarelli**, Presidente CLUSIT

12.15 Cocktail

Clusit

SECURITY SUMMIT

ASTREA

NIS2, dalle misure di base alla categorizzazione: guida ai prossimi passi del percorso di adeguamento.

29 aprile 2026

9.20 Apertura e moderazione dei lavori a cura di **Luca Bechelli**, CD CLUSIT

9.30 Intervento a cura di: **Milena Antonella Rizzi**, Capo Servizio Regolazione dell'**Agenzia per la Cybersicurezza Nazionale**

Interviene: **Claudio Telmon**, CD Clusit

11.00 Q&A

12.00 Conclusioni a cura di **Anna Vaccarelli**, Presidente CLUSIT

12.15 Cocktail

Contatti:

lbechelli@clusit.it
ctelmon@clusit.it
nis2@clusit.it