Nis2 - implementazione del decreto e prossimi passi

20/04/2026

Attuazione e ambito di applicazione

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

Ambito di applicazione

Settori, sottosettori e tipologie di soggetti introdotti dalla NIS2

[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	1 tipologia di soggetto			
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale				
Pubblica Amministrazione regionale e locale	11 categorie di PA			
Ulteriori tipologie di soggetti	4 tipologie e 2 criteri aggiuntivi	Identificazione dell'Autorità		

Autorità e Tavolo interministeriale

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

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)
- [Soggetti] Dal 1° gennaio al 28 febbraio di ogni anno, registrazione/aggiornamento
- [ACN] **Elaborazione del modello di categorizzazione delle attività e dei servizi**
- [ACN] Elaborazione obblighi a lungo termine

Da metà aprile 26

Terza fase attuativa

- **[Soggetti] Aggiornamento annuale delle informazioni (indicazione fornitori rilevanti)**
- [ACN] **Adozione del modello di categorizzazione delle attività e dei servizi (aprile 2026)**
- **[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

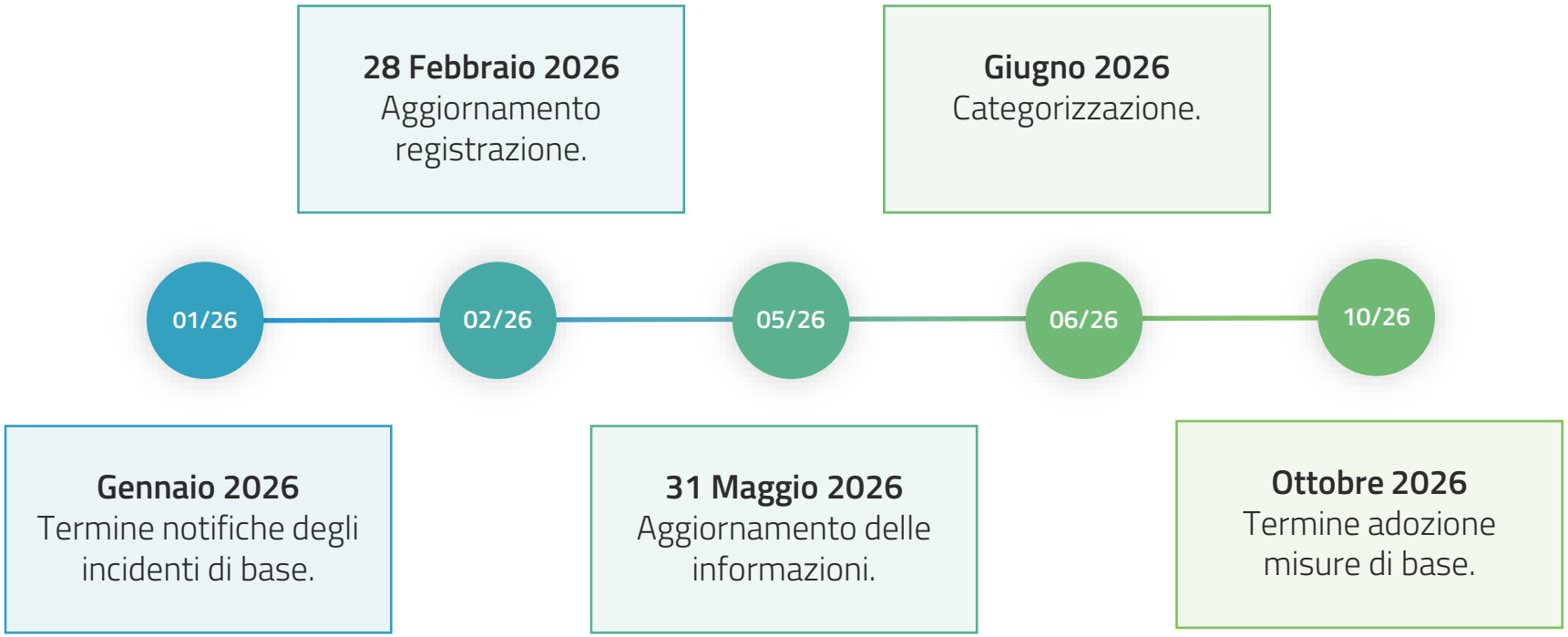

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

Obblighi

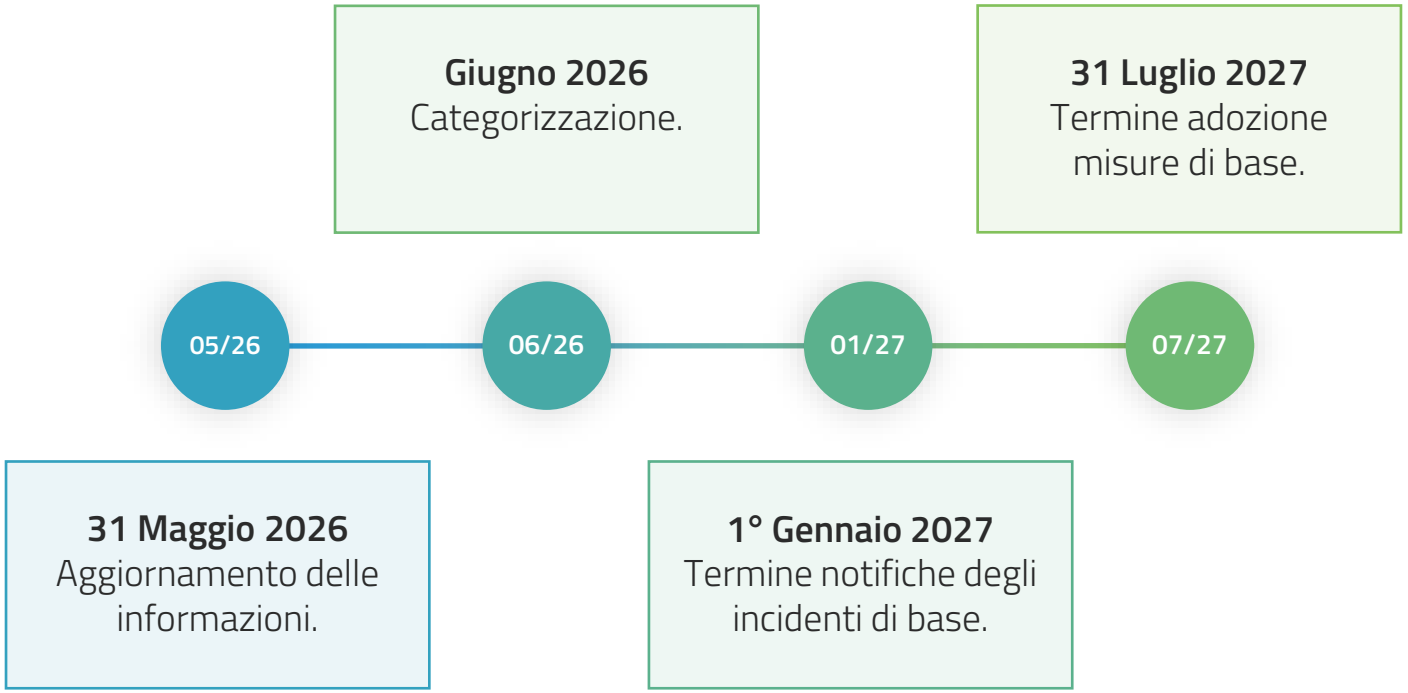
Elenco degli obblighi

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	Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi.

Calendario obblighi soggetti 2025 che permangono nell’elenco 2026



Calendario obblighi nuovi soggetti 2026



Aggiornamento delle informazioni

Aggiornamento continuo

- Tutte le informazioni devono essere aggiornate entro 14 giorni dalla modifica!

Conferma annuale

- Tutti gli anni, i soggetti devono confermare le informazioni conferite

Componenti degli organi di amministrazione e direttivi

- Sono i vertici dell'organizzazione
  i.e., Rappresentante legale, CDA (o equivalente) monocratico o collegiale, etc.
- Approvano e sovrintendono all'implementazione degli obblighi

Referente CSIRT

- Interloquisce con lo CSIRT Italia ed effettua le notifiche obbligatorie e volontarie
- Può essere coadiuvato da sostituti referenti CSIRT
- Possiede almeno competenze di base e conosce l'infrastruttura ICT del soggetto

Fornitori rilevanti

Fornitori rilevanti

Articolo 3, comma 9, lettera f):

Il presente decreto si applica, altresì, anche ai soggetti […], indipendentemente dalle loro dimensioni, individuati secondo le procedure di cui al comma 13, qualora: […] ***(f)*** *il soggetto sia considerato critico ai sensi del presente decreto quale elemento sistemico della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti*

Integrazioni alla Determinazione sulla piattaforma digitale NIS

CONSIDERATA la necessità di acquisire le informazioni relative ai fornitori considerati rilevanti al fine di individuare, ai sensi dell'articolo 3, comma 9, lettera f), del decreto NIS, gli elementi sistemici della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti;

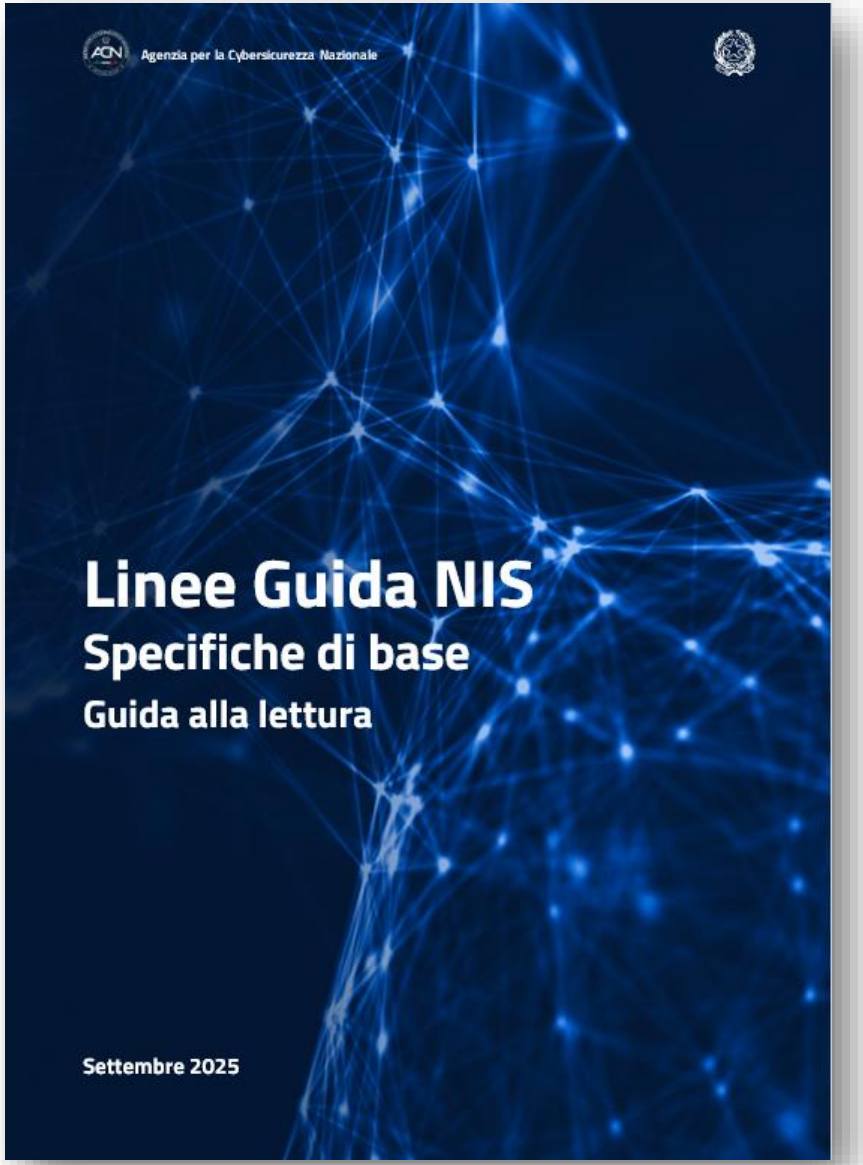
«fornitore rilevante NIS", un soggetto che assicura la fornitura di servizi o di prodotti a un soggetto NIS che soddisfa almeno uno dei seguenti criteri di rilevanza:

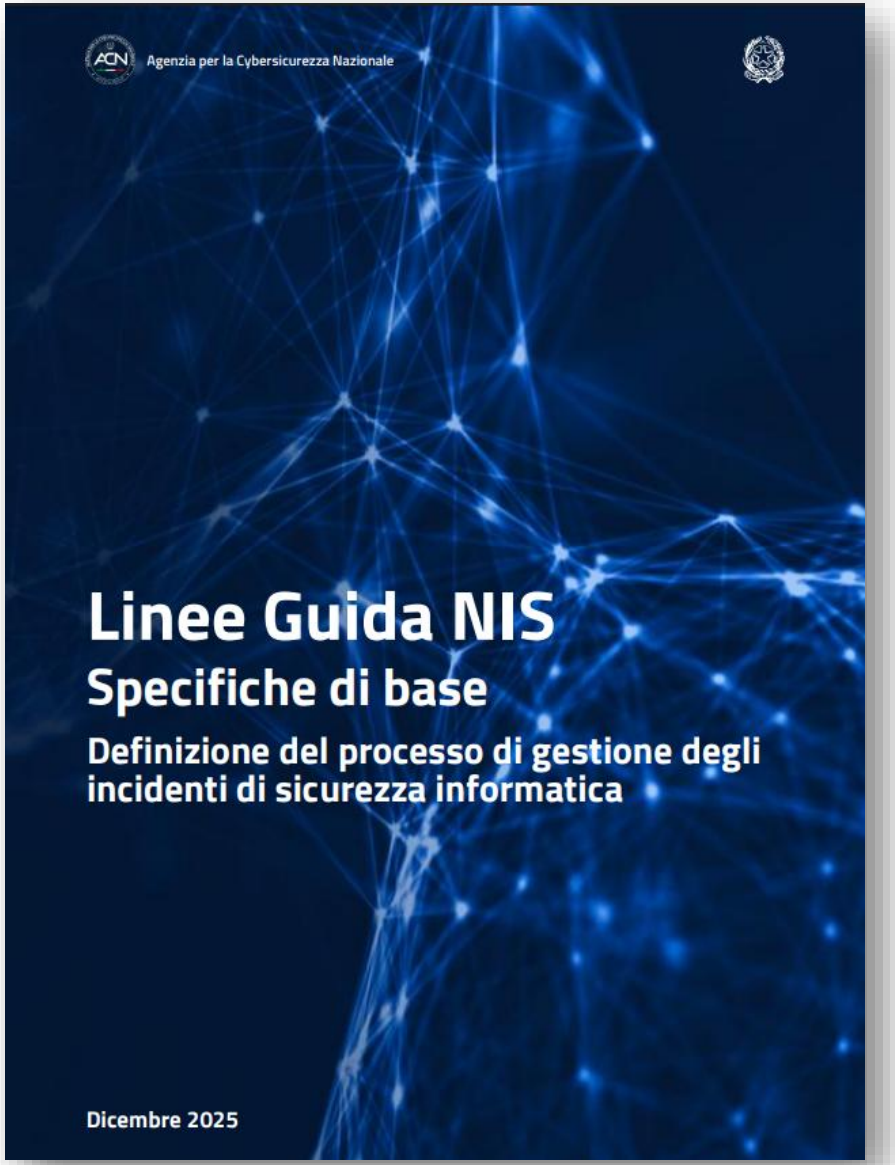
a) la fornitura è riconducibile alle attività o ai servizi di cui all'allegato I, punti 8 e 9, del decreto NIS (fornitura ICT);

b) l'interruzione o la compromissione della fornitura comporta un impatto significativo sulla capacità del soggetto NIS, anche per effetto della indisponibilità di fornitori alternativi, di erogare le attività o i servizi per i quali rientra nell'ambito di applicazione del decreto NIS (fornitura non fungibile);

Misure di sicurezza e notifiche di incidenti

Linee guida


Agenzia per la Cybersicurezza Nazionale
Linee Guida NIS
Specifiche di base
Guida alla lettura
Settembre 2025


Agenzia per la Cybersicurezza Nazionale
Linee Guida NIS
Specifiche di base
Definizione del processo di gestione degli incidenti di sicurezza informatica
Dicembre 2025

Misure di sicurezza di base (1/2)

Struttura misura

Codice | **Descrizione** | **Requisiti**

- Le misure sono organizzate in funzioni, categorie, sottocategorie e requisiti.
- Il codice identificativo (XX.YY-NN) e la descrizione della misura fanno riferimento al FNCDP ed.2025 (con il framework core allineato alle novità introdotte dal NIST con il CSF 2.0)
- I requisiti indicano ciò che è richiesto ai fini dell'implementazione.

Misure di sicurezza

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

Requisiti

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

Misure di sicurezza di base (2/2)

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.		●

Incidenti significativi di base

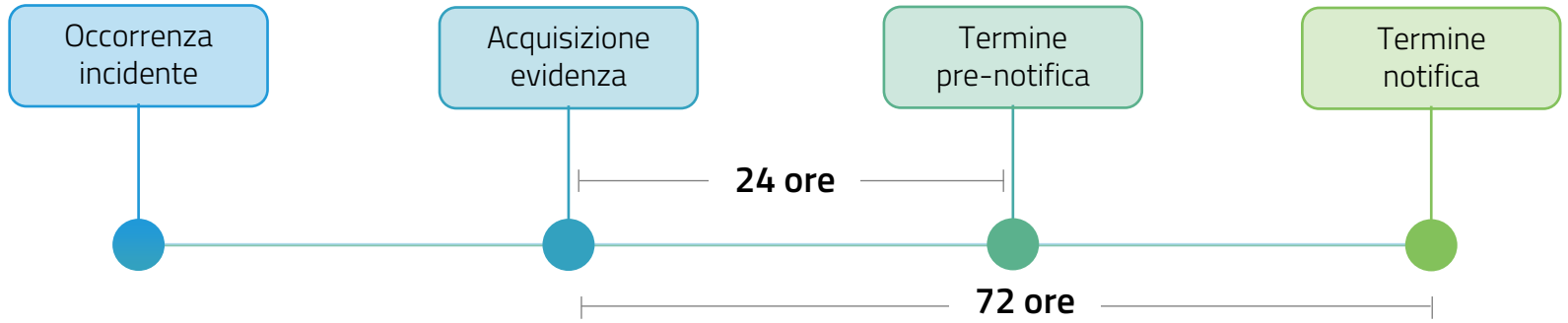
IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita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

Prossimi obblighi - Categorizzazione

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 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	Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi.

Implementazione articolo 30

L'agenzia stabilisce processo, modalità e criteri per elencazione, caratterizzazione e categorizzazione attività e servizi dei soggetti.

Definizione modello categorizzazione

Settembre 25 - Gennaio 26

L'agenzia può avvalersi dei tavoli settoriali ai fini di quanto previsto dall'articolo 30 del decreto NIS

Revisione modello categorizzazione

Febbraio 26

I soggetti comunicano e aggiornano elenco attività e servizi comprensivi di caratterizzazione e categoria di rilevanza.

Funzionalità su piattaforma online

Maggio 26- Giugno 26

Modello di categorizzazione (1/2)

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.

Soggetti privati e pubblici

- Differenziato a seconda che il soggetto NIS sia un soggetto privato o sia un soggetto della Pubblica Amministrazione.

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*.

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.

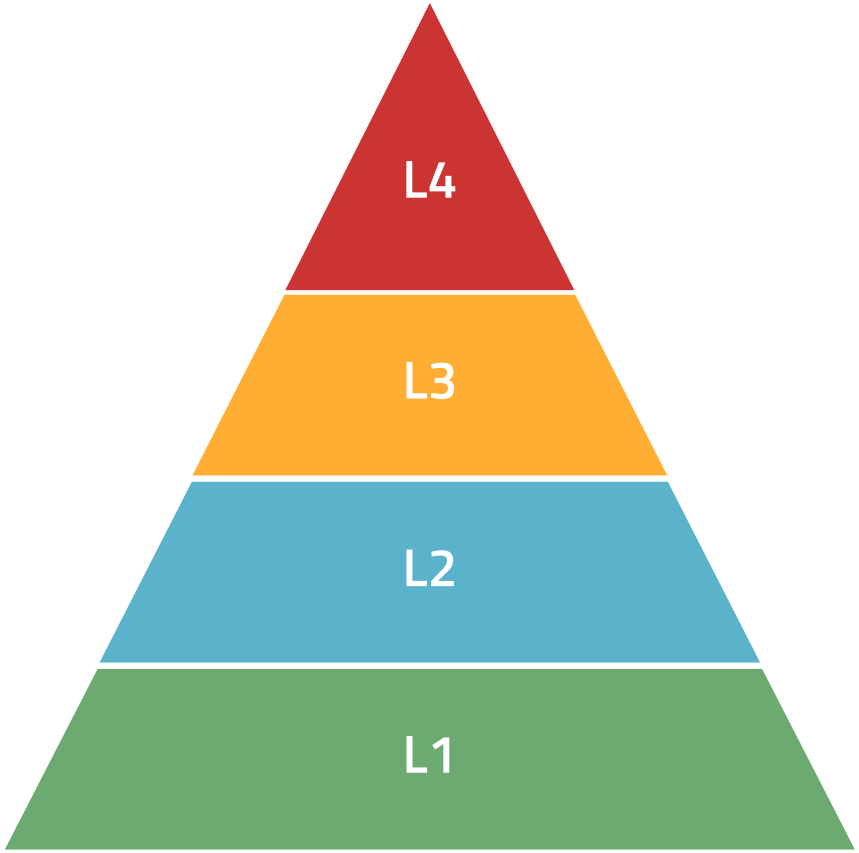
Categoria di rilevanza e misure di sicurezza (1/2)

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



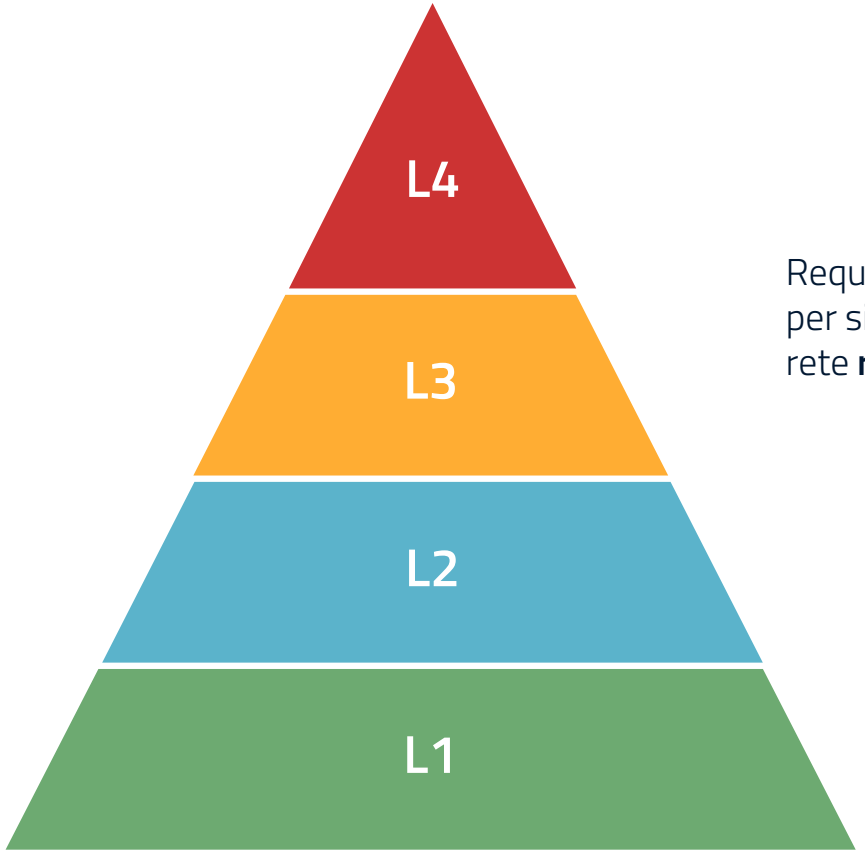
Sistemi informativi e di rete soggetti pubblici

- Reg. Cloud strategico
- Reg. Cloud critico
- Reg. Cloud ordinario
- Fuori ambito Reg. Cloud

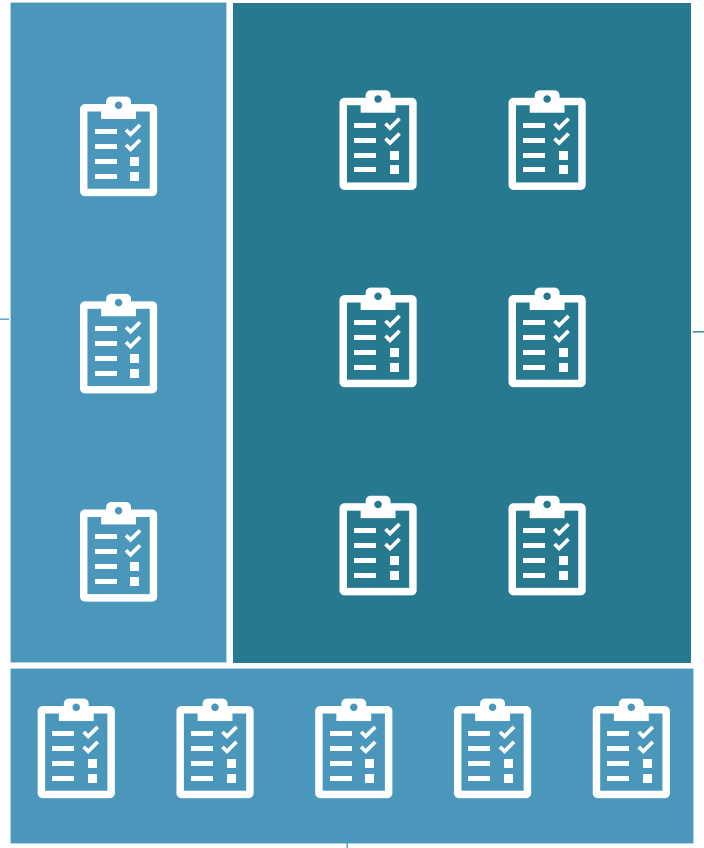
Categoria di rilevanza e misure di sicurezza (2/2)

Proposta su 4 livelli

Misure di sicurezza a lungo termine



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

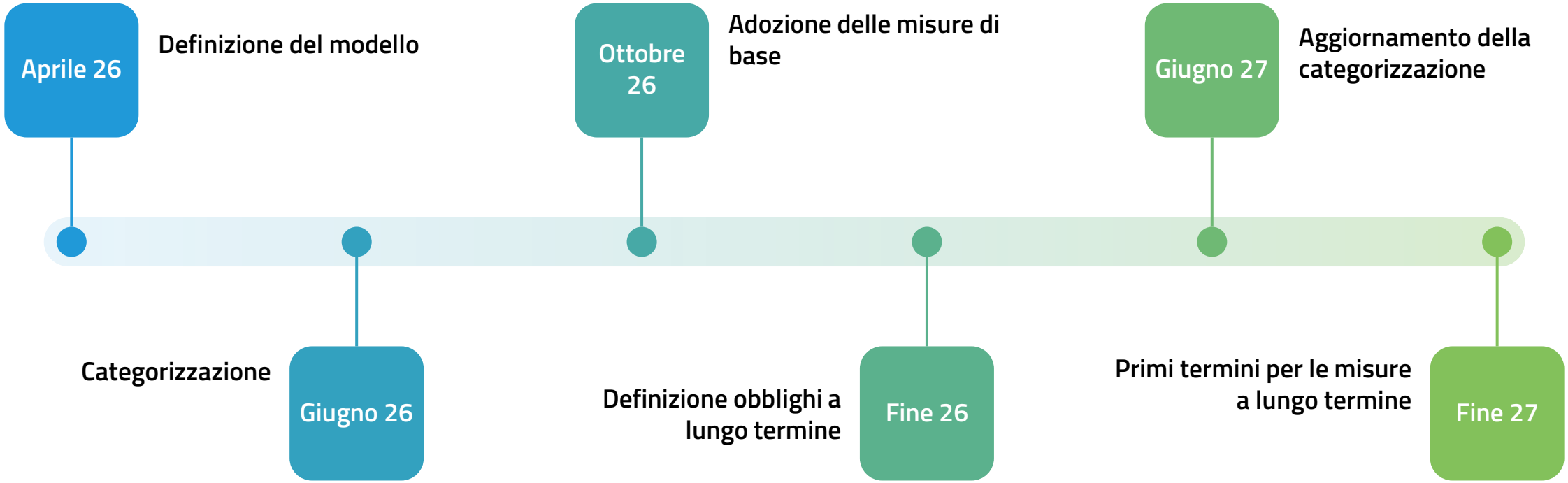


Requisiti **aggiuntivi**

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

Categorizzazione

In definizione



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 il settore pubblico

- Pubbliche Amministrazioni di cui all'allegato III
- Trasporto pubblico locale di cui all'allegato IV, partecipato o sottoposti a controllo pubblico
- Società in house, società partecipate e società a controllo pubblico non altrimenti individuate

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

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

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

https://www.acn.gov.it/portale/nis/modalita-specifiche-base

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