Perché siamo qui oggi

18 Novembre 2025

Responsabilità e obblighi

- 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

Nuova disciplina NIS

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 (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

Percorso di 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] 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

Governance

Autorità nazionale competente NIS (articolo 10)

Autorità nazionale competente NIS

- Sovrintende all'implementazione e all'attuazione del decreto NIS e predispone i provvedimenti
- Svolge le funzioni e le attività di regolamentazione, anche adottando linee guida, raccomandazioni e orientamenti non vincolanti
- Individua i soggetti essenziali e i soggetti importanti nonché **redige l'elenco dei soggetti NIS**;
- Partecipa al Gruppo di cooperazione NIS, nonché ai consessi e alle iniziative promosse a livello di Unione europea relativi all'attuazione della direttiva NIS2
- **Definisce gli obblighi in materia di registrazione** (art. 7), di **responsabilità degli organi di amministrazione e direttivi** (art. 23), di **misure di sicurezza** (art. 24), di **notifica di incidente** (art. 25) e di registrazione dei nomi di dominio (art. 29)
- Svolge le **attività di monitoraggio, analisi e supporto** (art. 35)
- Esercita i **poteri ispettivi** (art. 36), di **esecuzione** (art. 37) e **sanzionatori** (art. 38)

Autorità di settore NIS e Tavoli di settore (articolo 11)

Autorità di settore NIS

- **Verificano l'elenco dei soggetti NIS**
- **Supportano l'individuazione dei soggetti essenziali e dei soggetti importanti**
- Individuano i soggetti a cui si applicano le deroghe di cui all'articolo 3, comma 4;
- Supportano le funzioni e le attività di regolamentazione
- Elaborano dei contributi per la relazione annuale
- **Istituiscono e coordinano i tavoli settoriali**, al fine di contribuire **all'efficace e coerente attuazione settoriale** del decreto NIS nonché al relativo **monitoraggio**.
- Partecipano alle attività settoriali del Gruppo di Cooperazione NIS

Tavoli di settore

- **Camera di compensazione e confronto con i settori/soggetti NIS** per una efficace attuazione della disciplina
- Individuazione di criticità e condivisione di approcci in fase legislativa e regolamentare
- Monitoraggio dell’attuazione

Tavolo NIS

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

Registrazione – Esiti

Oltre 30K organizzazioni censite

Oltre 20K soggetti NIS

Oltre 5K soggetti essenziali

Oltre 7K ticket evasi

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

Specifiche di base

Base giuridica

D.Lgs. 138/2024

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 164179/2025

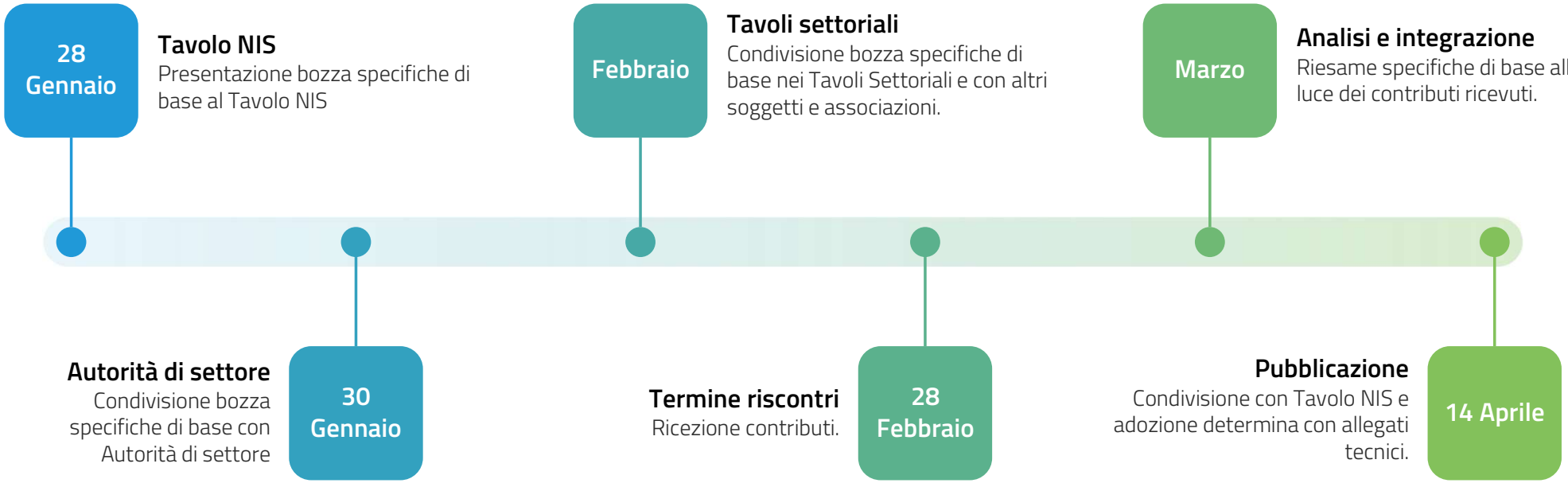
Allegato 1
Misure di sicurezza di base soggetti importanti

Allegato 2
Misure di sicurezza di base soggetti essenziali

Allegato 3
Incidenti significativi di base soggetti importanti

Allegato 4
Incidenti significativi di base soggetti importanti

Processo di adozione



Regime transitorio*

Determinazione 164179 del 14/04

Ex OSE (Dlgs 65/2018)

Nelle more di adottare le specifiche di base su tutta l'infrastruttura entro 18 mesi dalla ricezione della comunicazione di inserimento nell'elenco dei soggetti NIS [generalmente ottobre 2026]

- ❑ Mantengono le misure di sicurezza già implementate ai sensi del dlgs 65/2018 sulla porzione di infrastruttura che abilitata l'erogazione dei servizi essenziali
- ❑ Proseguono a effettuare le notifiche nel nuovo contesto NIS

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.

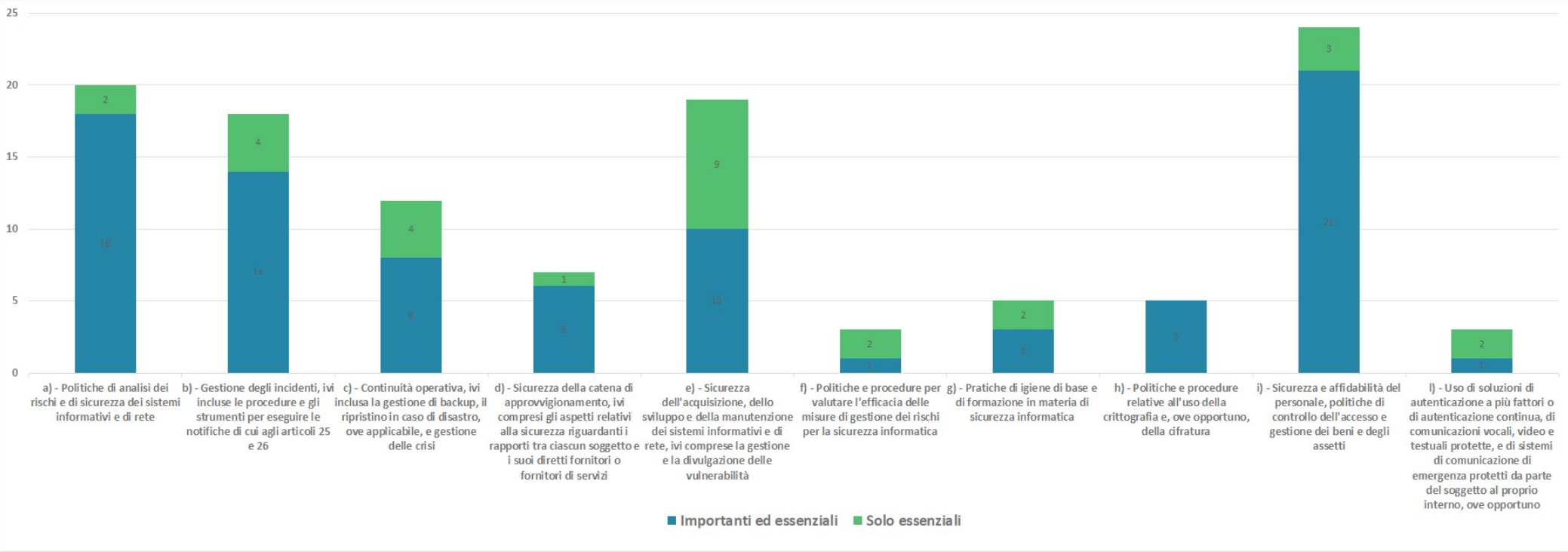
Misure di sicurezza

Elementi misure di sicurezza

a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi.	b) Gestione degli incidenti.	c) Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi.	d) Sicurezza catena di approvvigionamento, compresi aspetti relativi sicurezza rapporti con diretti fornitori o fornitori di servizi.	e) Sicurezza acquisizione, sviluppo e manutenzione sistemi informativi e di rete, ivi compresa gestione e divulgazione vulnerabilità.
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza.	g) Pratiche di igiene informatica di base e formazione in materia di cybersicurezza.	h) Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura.	i) Sicurezza risorse umane, strategie di controllo dell'accesso e gestione degli assetti.	j) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti.

Elementi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica (art. 24, c. 2 d.lgs. 138/2024)

Mappatura requisiti – elementi art. 24, co. 2, decreto NIS



Quadro generale

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.

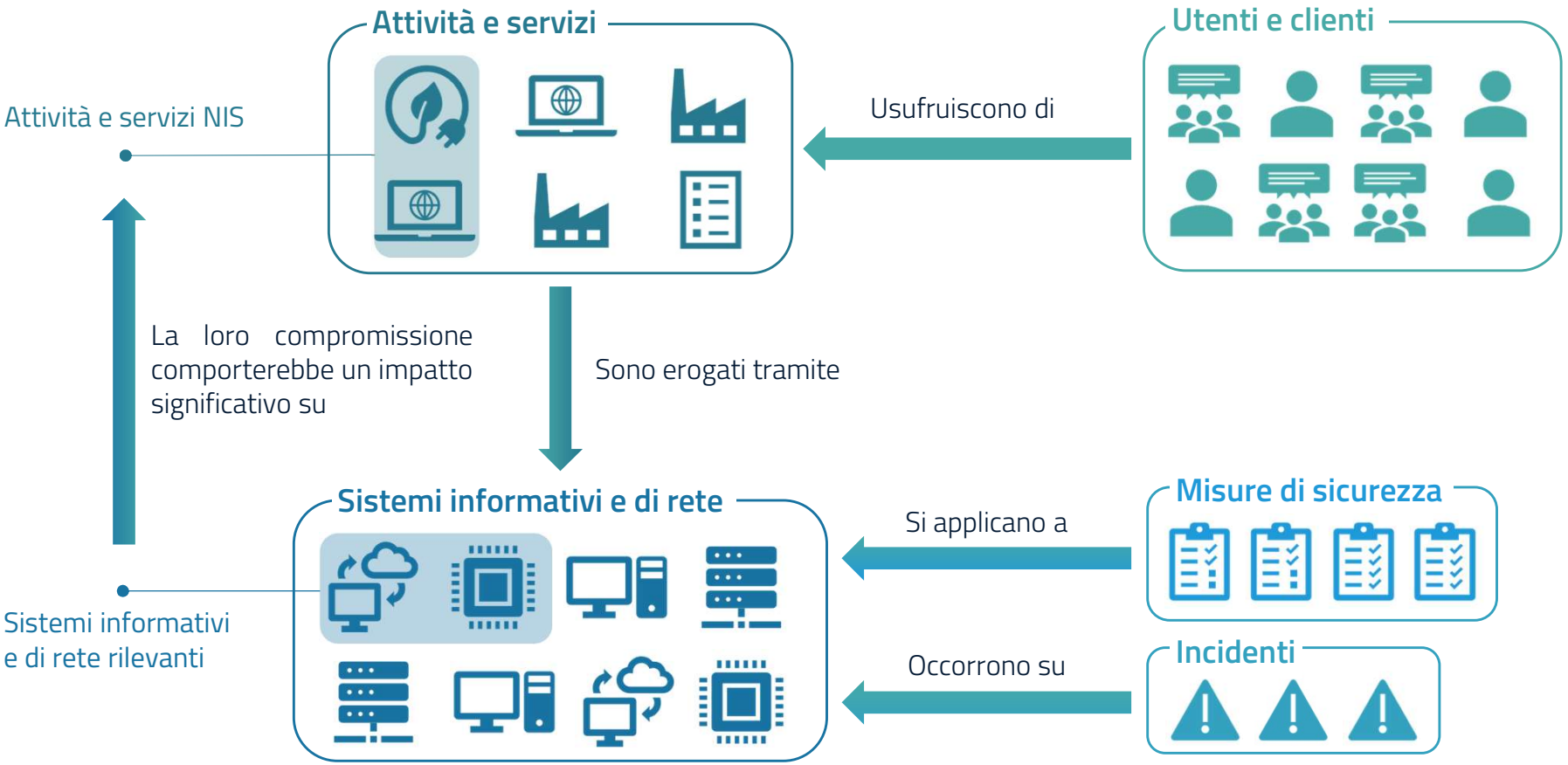
Misure di sicurezza

- **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.

Ambito di applicazione



Approccio basato sul rischio

Ambito

Le misure di sicurezza si applicano a tutti i sistemi informativi e di rete del soggetto.

Livello di rischio

Ogni sistema informativo e di rete è caratterizzato da un proprio livello di rischio.

Proporzionalità

L'art. 31 del decreto prevede che si tenga conto, nello stabilire gli obblighi, del grado di esposizione dei soggetti ai rischi.

Approccio

Le misure di sicurezza sono state sviluppate secondo un approccio basato sul rischio.

Clausole

Previsione per i requisiti di maggiore complessità di specifiche clausole.

Declinazione approccio basato sul rischio

14 requisiti per i soggetti importanti
e **19** per i soggetti essenziali

6 requisiti per i soggetti importanti
e **9** per i soggetti essenziali

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 delle attività e servizi per i quali il soggetto rientra nell'ambito di applicazione del decreto NIS.

“ ... per almeno i sistemi informativi e di rete rilevanti ... ”

“ ... in accordo agli esiti della della valutazione del rischio di cui alla misura ... ”

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.

“ ... fatte salve motivate e documentate ragioni normative o tecniche ... ”

“ ... forniture con potenziali impatti sulla sicurezza ... ”

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

8 requisiti per i soggetti importanti
e **10** per i soggetti essenziali

3 requisiti per i soggetti importanti
e per i soggetti essenziali

Sistemi informativi e di rete rilevanti

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.		●

In accordo a esiti valutazione rischio

PR.AA-01

Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.

PUNTO	REQUISITO	S_I	S_E
1	Tutte le utenze, ivi incluse quelle con privilegi amministrativi e quelle utilizzate per l'accesso remoto, sono censite, approvate da attori interni al soggetto NIS e, fatte salve motivate e documentate ragioni tecniche, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono individuali per gli utenti.	●	●
2	Le credenziali (ad esempio nome utente e password) relative alle utenze sono robuste e aggiornate in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05.	●	●
3	Per almeno i sistemi informativi e di rete rilevanti, sono verificate periodicamente le utenze e le relative autorizzazioni, aggiornandole/revocandole in caso di variazioni (ad esempio trasferimento o cessazione di personale).	●	●
4	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1, 2 e 3.	●	●

PR.AA-03

Utenti, servizi e hardware sono autenticati

PUNTO	REQUISITO	S_I	S_E
1	Le modalità di autenticazione delle utenze per accedere ai sistemi informativi e di rete sono commisurate al rischio. A tal fine sono valutati almeno i rischi connessi: a) ai privilegi delle utenze; b) alla criticità dei sistemi informativi e di rete; c) alla tipologia di operazioni che le utenze possono effettuare sui sistemi informativi e di rete.	●	●
2	Per almeno i sistemi informativi e di rete rilevanti e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono impiegate modalità di autenticazione multifattore.	●	●
3	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.	●	●

Fatte salve motivate e documentate ragioni

DE.CM-09

L'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati sono monitorati per individuare eventi potenzialmente avversi.

PUNTO	REQUISITO	S_I	S_E
1	Fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato, sistemi di protezione delle postazioni terminali per il rilevamento del codice malevolo.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●

Forniture con potenziali impatti sulla sicurezza

GV.SC-01

Sono stabiliti e accettati dagli stakeholder dell'organizzazione il programma, la strategia, obiettivi, politiche e processi di gestione del rischio di cybersecurity della catena di approvvigionamento.

PUNTO	REQUISITO	S_I	S_E
1	In merito all'affidamento di forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, anche mediante ricorso agli strumenti delle centrali di committenza di cui all'allegato I.1, articolo 1, comma 1, lettera i), del decreto legislativo 31 marzo 2023, n. 36, sono previsti: a) il coinvolgimento dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02 nella definizione ed esecuzione dei processi di approvvigionamento a partire dalla fase di identificazione e progettazione della fornitura; b) in accordo agli esiti della valutazione del rischio associato alla fornitura di cui alla misura GV.SC-07, la definizione di requisiti di sicurezza sulla fornitura coerenti con le misure di sicurezza applicate dal soggetto NIS ai sistemi informativi e di rete.	●	●

Tipologia requisiti

Specifiche amministrative

Ad esempio:

- Adozione e approvazione politiche e procedure.
- Definizione di piani (ad es. risposta agli incidenti)
- Redazione documentazione.

Specifiche tecniche

Ad esempio:

- Cifratura dei dati.
- Aggiornamento del software.
- Modalità di autenticazione multifattore.

Evidenze documentali

Elenchi

Personale dell'organizzazione di sicurezza informatica, *configurazioni di riferimento*, sistemi ai quali è possibile accedere da remoto.

Inventari

Apparati fisici, servizi, sistemi e applicazioni software, *flussi di rete*, servizi erogati dai fornitori, fornitori

Piani

Gestione del rischio, business continuity e disaster recovery, trattamento del rischio, gestione delle vulnerabilità, adeguamento, *valutazione dell'efficacia delle misure di gestione del rischio*, formazione in materia di sicurezza informatica, risposta agli incidenti

Politiche

definite per almeno i requisiti riportati nella tabella 1 in appendice all'Allegato 1, per i soggetti importanti, e all'allegato 2, per i soggetti essenziali, della determina 164179/2025

Procedure

In relazione agli specifici requisiti per i quali sono richieste.

Registri

Esiti del riesame delle politiche, attività formazione dei dipendenti, *manutenzioni effettuate*.

Incidenti significativi

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

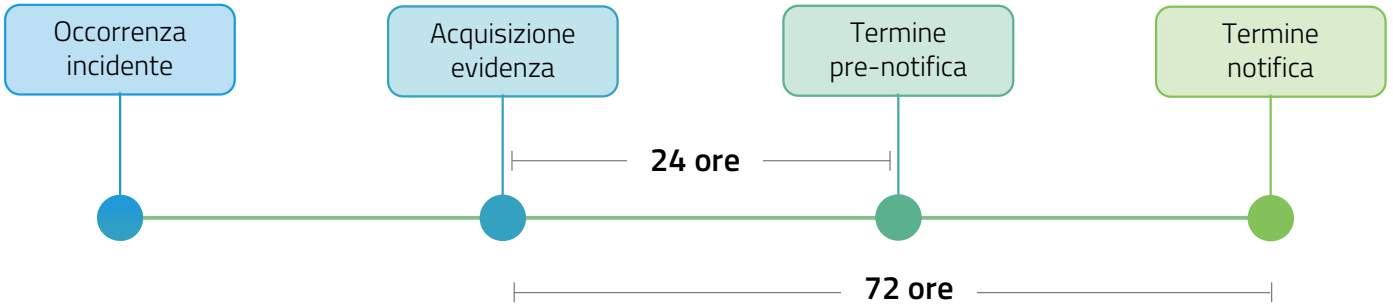
Solo soggetti essenziali
1 tipologia di incidente

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

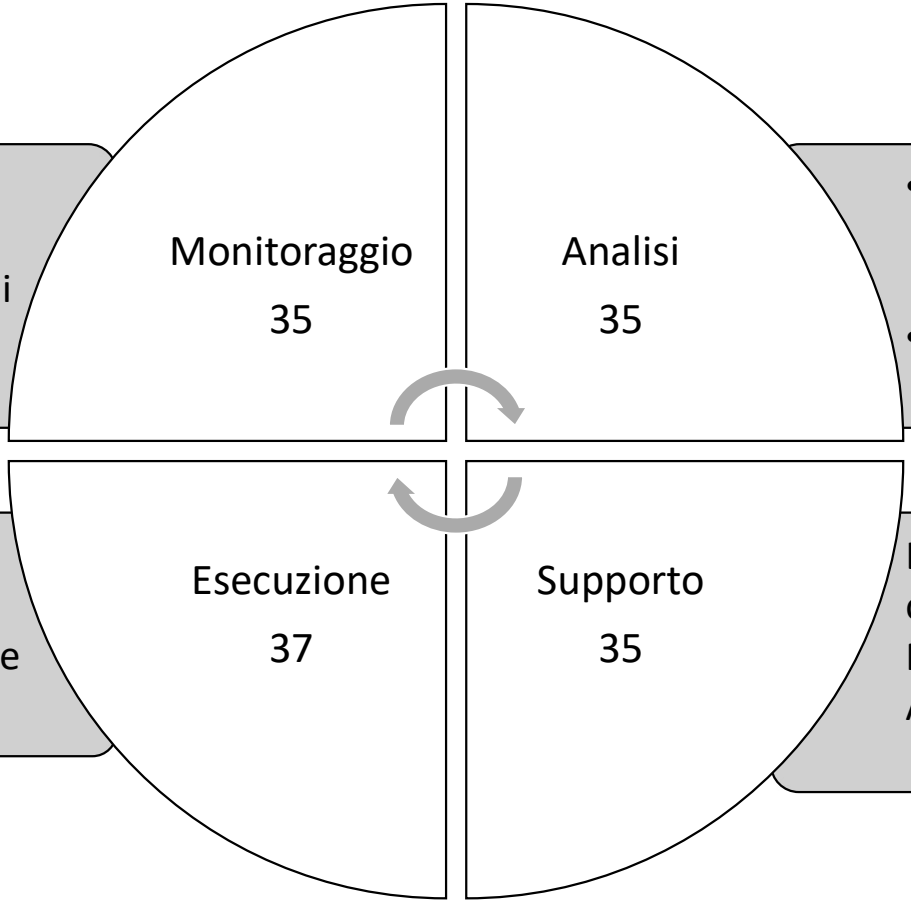
Fattispecie in cui un operatore abbia l'autorizzazione tecnica (ossia la disponibilità di credenziali che sono configurate per accedere ai dati) per accedere a determinati dati ma tale acceso sia effettivamente illecito in quanto, ad esempio, effettuato in violazione delle politiche del soggetto o risulti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

Monitoraggio, analisi e supporto

Poteri di esecuzione

Monitoraggio, analisi e supporto (articolo 35) + Poteri di esecuzione (articolo 37)

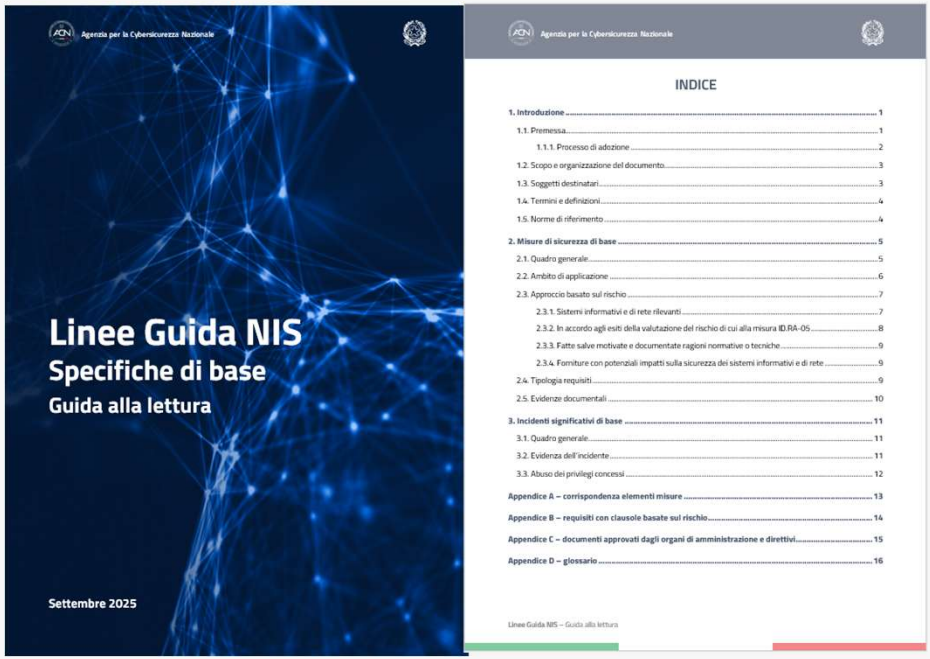
- Acquisizione dello stato di attuazione degli obblighi
- Anche tramite il Tavolo NIS, i Tavoli settoriali e rendicontazioni periodiche



- Individuazione di criticità e soluzioni, sistemiche o individuali
- Anche tramite il Tavolo NIS e i Tavoli settoriali

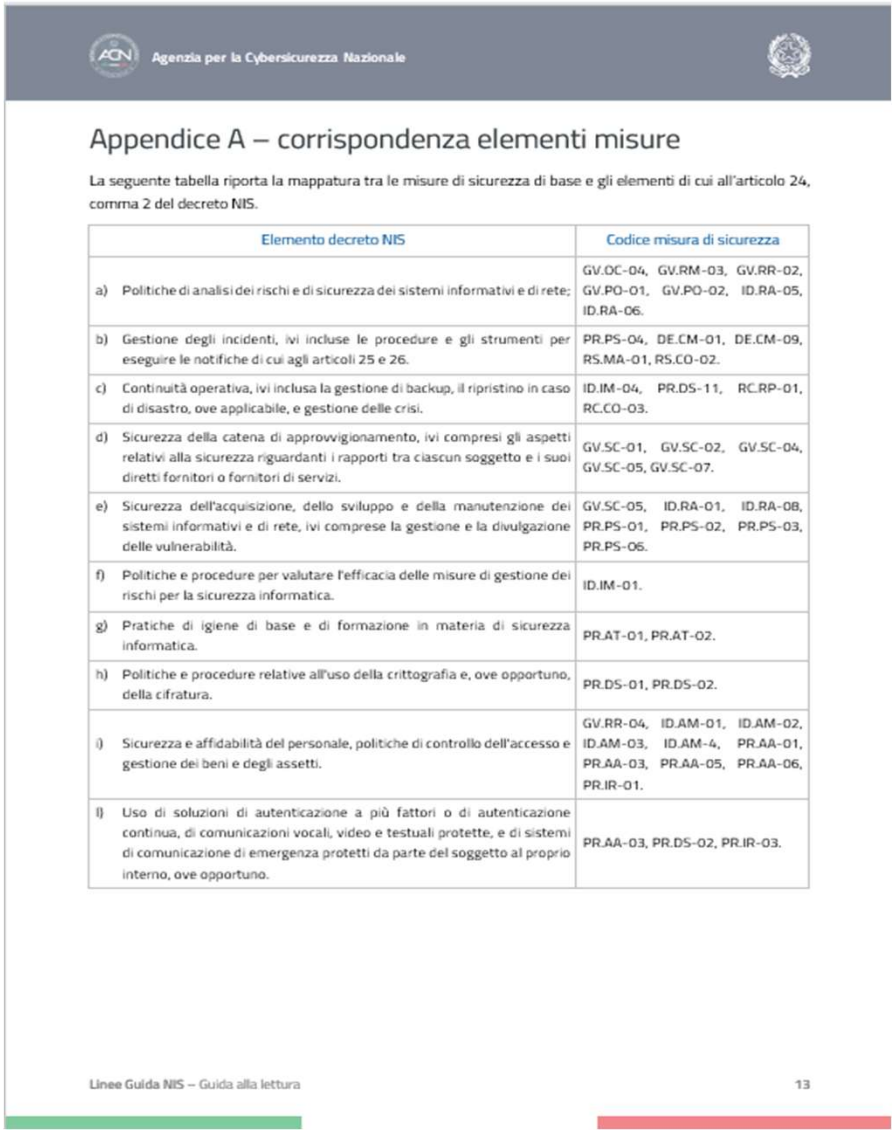
Imposizione di audit di terze parti
Intimazione di attuare istruzioni vincolanti o di porre rimedio a carenze
Diffida

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



Linee Guida NIS – Specifiche di base – Guida alla lettura

Appendici 1/4



Agenzia per la Cybersicurezza Nazionale

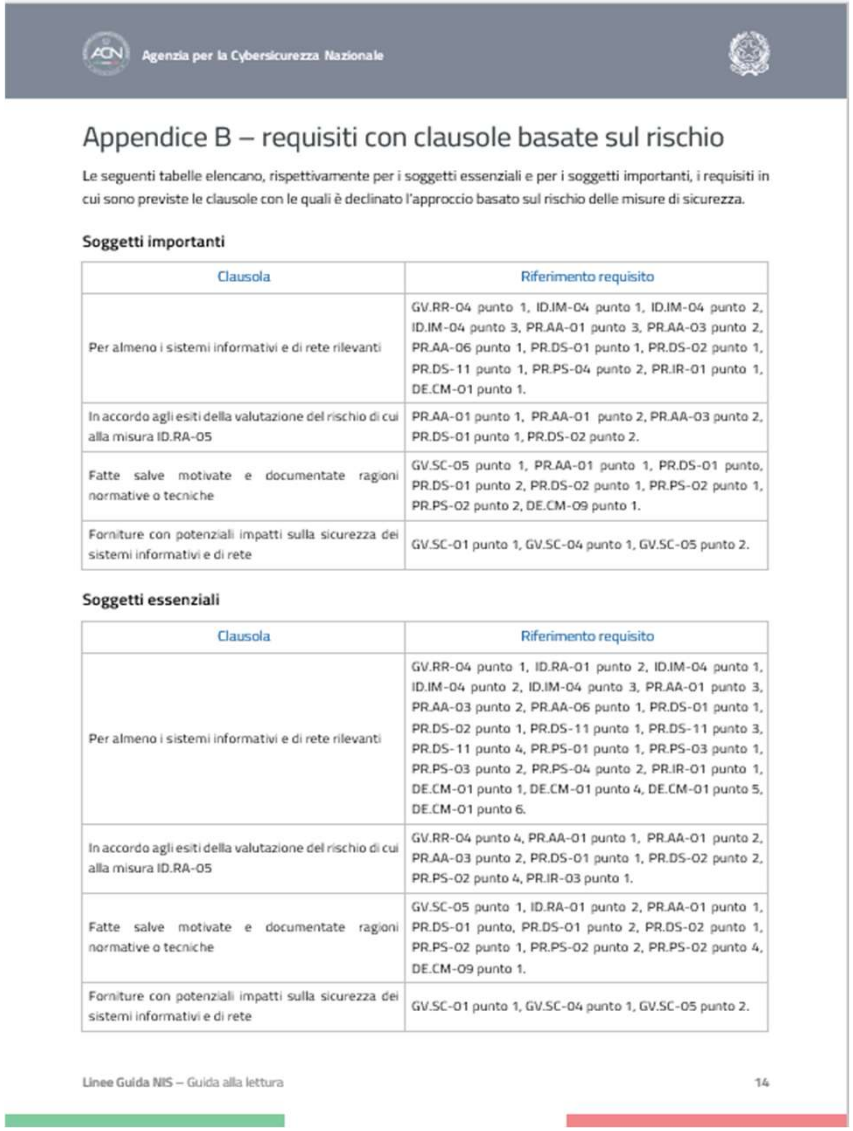
Appendice A – corrispondenza elementi misure

La seguente tabella riporta la mappatura tra le misure di sicurezza di base e gli elementi di cui all'articolo 24, comma 2 del decreto NIS.

Elemento decreto NIS	Codice misura di sicurezza
a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;	GV.OC-04, GV.RM-03, GV.RR-02, GV.PO-01, GV.PO-02, ID.RA-05, ID.RA-06.
b) Gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26.	PR.PS-04, DE.CM-01, DE.CM-09, RS.MA-01, RS.CO-02.
c) Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi.	ID.IM-04, PR.DS-11, RC.RP-01, RC.CO-03.
d) Sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi.	GV.SC-01, GV.SC-02, GV.SC-04, GV.SC-05, GV.SC-07.
e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità.	GV.SC-05, ID.RA-01, ID.RA-08, PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-06.
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica.	ID.IM-01.
g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica.	PR.AT-01, PR.AT-02.
h) Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura.	PR.DS-01, PR.DS-02.
i) Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti.	GV.RR-04, ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-4, PR.AA-01, PR.AA-03, PR.AA-05, PR.AA-06, PR.IR-01.
l) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.	PR.AA-03, PR.DS-02, PR.IR-03.

Linee Guida NIS – Guida alla lettura 13

Appendici 2/4



Appendice B – requisiti con clausole basate sul rischio

Le seguenti tabelle elencano, rispettivamente per i soggetti essenziali e per i soggetti importanti, i requisiti in cui sono previste le clausole con le quali è declinato l'approccio basato sul rischio delle misure di sicurezza.

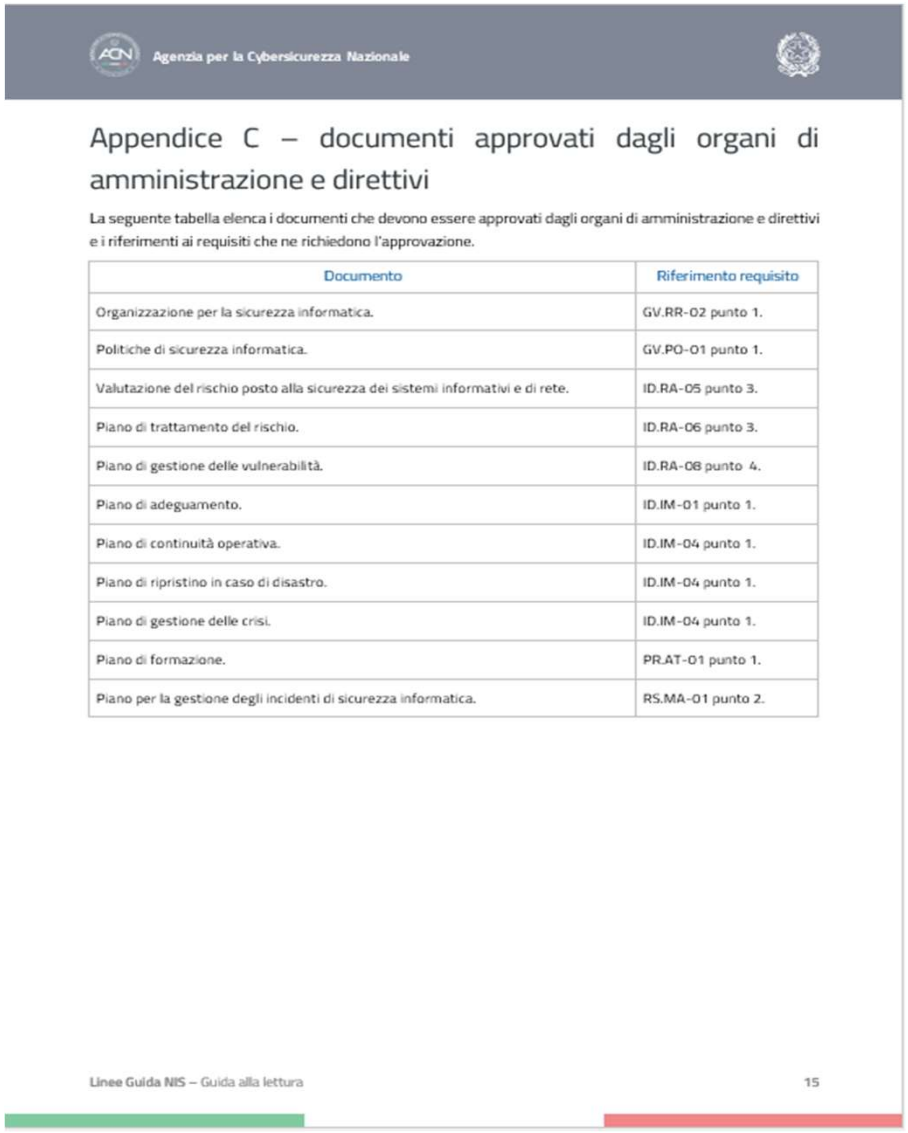
Soggetti importanti

Clausola	Riferimento requisito
Per almeno i sistemi informativi e di rete rilevanti	GV.RR-04 punto 1, ID.IM-04 punto 1, ID.IM-04 punto 2, ID.IM-04 punto 3, PR.AA-01 punto 3, PR.AA-03 punto 2, PR.AA-06 punto 1, PR.DS-01 punto 1, PR.DS-02 punto 1, PR.DS-11 punto 1, PR.PS-04 punto 2, PR.IR-01 punto 1, DE.CM-01 punto 1.
In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05	PR.AA-01 punto 1, PR.AA-01 punto 2, PR.AA-03 punto 2, PR.DS-01 punto 1, PR.DS-02 punto 2.
Fatte salve motivate e documentate ragioni normative o tecniche	GV.SC-05 punto 1, PR.AA-01 punto 1, PR.DS-01 punto, PR.DS-01 punto 2, PR.DS-02 punto 1, PR.PS-02 punto 1, PR.PS-02 punto 2, DE.CM-09 punto 1.
Forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete	GV.SC-01 punto 1, GV.SC-04 punto 1, GV.SC-05 punto 2.

Soggetti essenziali

Clausola	Riferimento requisito
Per almeno i sistemi informativi e di rete rilevanti	GV.RR-04 punto 1, ID.RA-01 punto 2, ID.IM-04 punto 1, ID.IM-04 punto 2, ID.IM-04 punto 3, PR.AA-01 punto 3, PR.AA-03 punto 2, PR.AA-06 punto 1, PR.DS-01 punto 1, PR.DS-02 punto 1, PR.DS-11 punto 1, PR.DS-11 punto 3, PR.DS-11 punto 4, PR.PS-01 punto 1, PR.PS-03 punto 1, PR.PS-03 punto 2, PR.PS-04 punto 2, PR.IR-01 punto 1, DE.CM-01 punto 1, DE.CM-01 punto 4, DE.CM-01 punto 5, DE.CM-01 punto 6.
In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05	GV.RR-04 punto 4, PR.AA-01 punto 1, PR.AA-01 punto 2, PR.AA-03 punto 2, PR.DS-01 punto 1, PR.DS-02 punto 2, PR.PS-02 punto 4, PR.IR-03 punto 1.
Fatte salve motivate e documentate ragioni normative o tecniche	GV.SC-05 punto 1, ID.RA-01 punto 2, PR.AA-01 punto 1, PR.DS-01 punto, PR.DS-01 punto 2, PR.DS-02 punto 1, PR.PS-02 punto 1, PR.PS-02 punto 2, PR.PS-02 punto 4, DE.CM-09 punto 1.
Forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete	GV.SC-01 punto 1, GV.SC-04 punto 1, GV.SC-05 punto 2.

Appendici 3/4

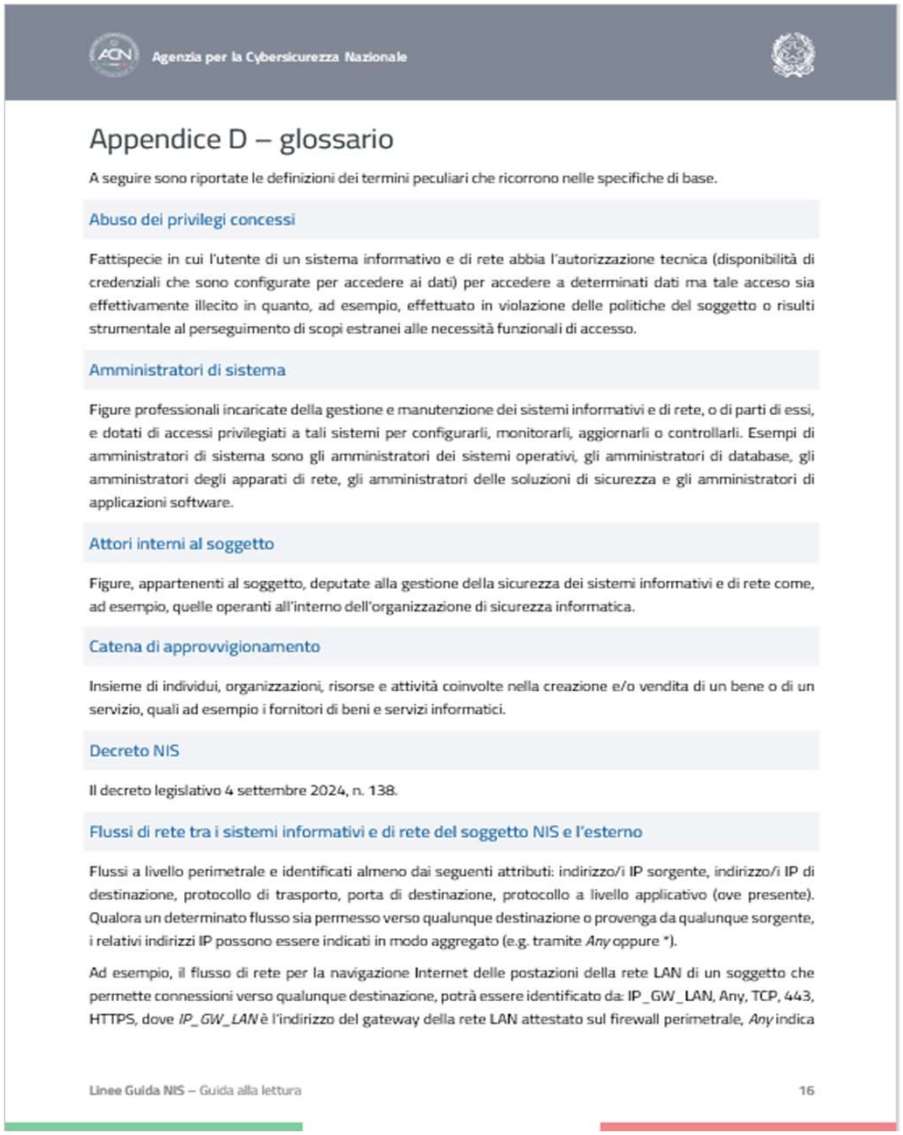


Appendice C – documenti approvati dagli organi di amministrazione e direttivi

La seguente tabella elenca i documenti che devono essere approvati dagli organi di amministrazione e direttivi e i riferimenti ai requisiti che ne richiedono l'approvazione.

Documento	Riferimento requisito
Organizzazione per la sicurezza informatica.	GV.RR-02 punto 1.
Politiche di sicurezza informatica.	GV.PO-01 punto 1.
Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete.	ID.RA-05 punto 3.
Piano di trattamento del rischio.	ID.RA-06 punto 3.
Piano di gestione delle vulnerabilità.	ID.RA-08 punto 4.
Piano di adeguamento.	ID.IM-01 punto 1.
Piano di continuità operativa.	ID.IM-04 punto 1.
Piano di ripristino in caso di disastro.	ID.IM-04 punto 1.
Piano di gestione delle crisi.	ID.IM-04 punto 1.
Piano di formazione.	PR.AT-01 punto 1.
Piano per la gestione degli incidenti di sicurezza informatica.	RS.MA-01 punto 2.

Appendici 4/4



Agenzia per la Cybersicurezza Nazionale

Appendice D – glossario

A seguire sono riportate le definizioni dei termini peculiari che ricorrono nelle specifiche di base.

Abuso dei privilegi concessi

Fattispecie in cui l'utente di un sistema informativo e di rete abbia l'autorizzazione tecnica (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.

Amministratori di sistema

Figure professionali incaricate della gestione e manutenzione dei sistemi informativi e di rete, o di parti di essi, e dotati di accessi privilegiati a tali sistemi per configurarli, monitorarli, aggiornarli o controllarli. Esempi di amministratori di sistema sono gli amministratori dei sistemi operativi, gli amministratori di database, gli amministratori degli apparati di rete, gli amministratori delle soluzioni di sicurezza e gli amministratori di applicazioni software.

Attori interni al soggetto

Figure, appartenenti al soggetto, deputate alla gestione della sicurezza dei sistemi informativi e di rete come, ad esempio, quelle operanti all'interno dell'organizzazione di sicurezza informatica.

Catena di approvvigionamento

Insieme di individui, organizzazioni, risorse e attività coinvolte nella creazione e/o vendita di un bene o di un servizio, quali ad esempio i fornitori di beni e servizi informatici.

Decreto NIS

Il decreto legislativo 4 settembre 2024, n. 138.

Flussi di rete tra i sistemi informativi e di rete del soggetto NIS e l'esterno

Flussi a livello perimetrale e identificati almeno dai seguenti attributi: indirizzo/i IP sorgente, indirizzo/i IP di destinazione, protocollo di trasporto, porta di destinazione, protocollo a livello applicativo (ove presente). Qualora un determinato flusso sia permesso verso qualunque destinazione o provenga da qualunque sorgente, i relativi indirizzi IP possono essere indicati in modo aggregato (e.g. tramite *Any* oppure *).

Ad esempio, il flusso di rete per la navigazione Internet delle postazioni della rete LAN di un soggetto che permette connessioni verso qualunque destinazione, potrà essere identificato da: IP_GW_LAN, Any, TCP, 443, HTTPS, dove *IP_GW_LAN* è l'indirizzo del gateway della rete LAN attestato sul firewall perimetrale, *Any* indica

Linee Guida NIS – Guida alla lettura 16

Prossimi passi

Scadenze

Notifiche degli incidenti significativi di base
- Gennaio 2026

Aggiornamento registrazione (2026)
- Febbraio 2026

Aggiornamento delle informazioni (2026)
- Maggio 2026

Categorizzazione (2026)
- Giugno 2026

Misure di sicurezza di base
- Ottobre 2026

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

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

https://www.acn.gov.it/portale/documents/d/guest/detacn_nis_piattaforma_2024_38565_signed

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

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

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