Security Summit Manifacturing
Focus NIS2

5 NOVEMBRE 2025

Decreto Legislativo NIS

Ambito di applicazione e attuazione

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		Identificazione dell'Autorità		
Pubblica Amministrazione regionale e locale	11 categorie di PA			
Ulteriori tipologie di soggetti	4 tipologie e 2 criteri aggiuntivi			

Recepimento e attuazione

Febbraio 23 - metà ottobre 24

Recepimento

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

Metà ottobre 24 - metà aprile 25

Prima fase attuativa

- [ACN e Autorità di settore] Avvio formale di tutti i tavoli settoriali
- **[Soggetti]** Censimento e registrazione dei soggetti (entro febbraio 2025)
- [ACN e Autorità di settore] **Adozione dell'elenco dei soggetti NIS e notifica (aprile 2025)**
- [ACN] **Elaborazione e adozione degli obblighi di base (aprile 2025)**

Metà aprile 25 - metà ottobre 26

Seconda fase attuativa

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

Da metà aprile 26

Terza fase attuativa

- **[Soggetti] Completamento dell'implementazione obblighi di base** (termine per misure di sicurezza 10/2026**)**
- [Soggetti] Categorizzazione delle attività e dei servizi
- [Soggetti] Implementazione degli obblighi a lungo termine

Obblighi di base

Misure di sicurezza e tassonomia incidenti.

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

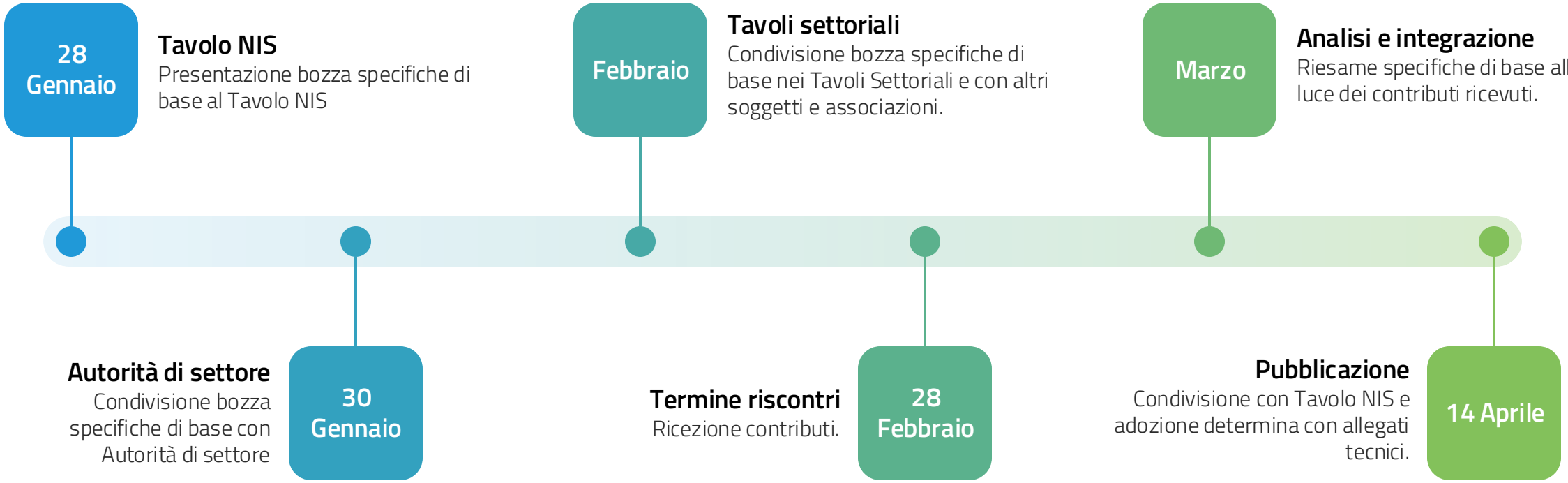
Allegato 1
Misure di sicurezza di base soggetti importanti

Allegato 2
Misure di sicurezza di base soggetti essenziali

Allegato 3
Incidenti significativi di base soggetti importanti

Allegato 4
Incidenti significativi di base soggetti essenziali

Processo di adozione



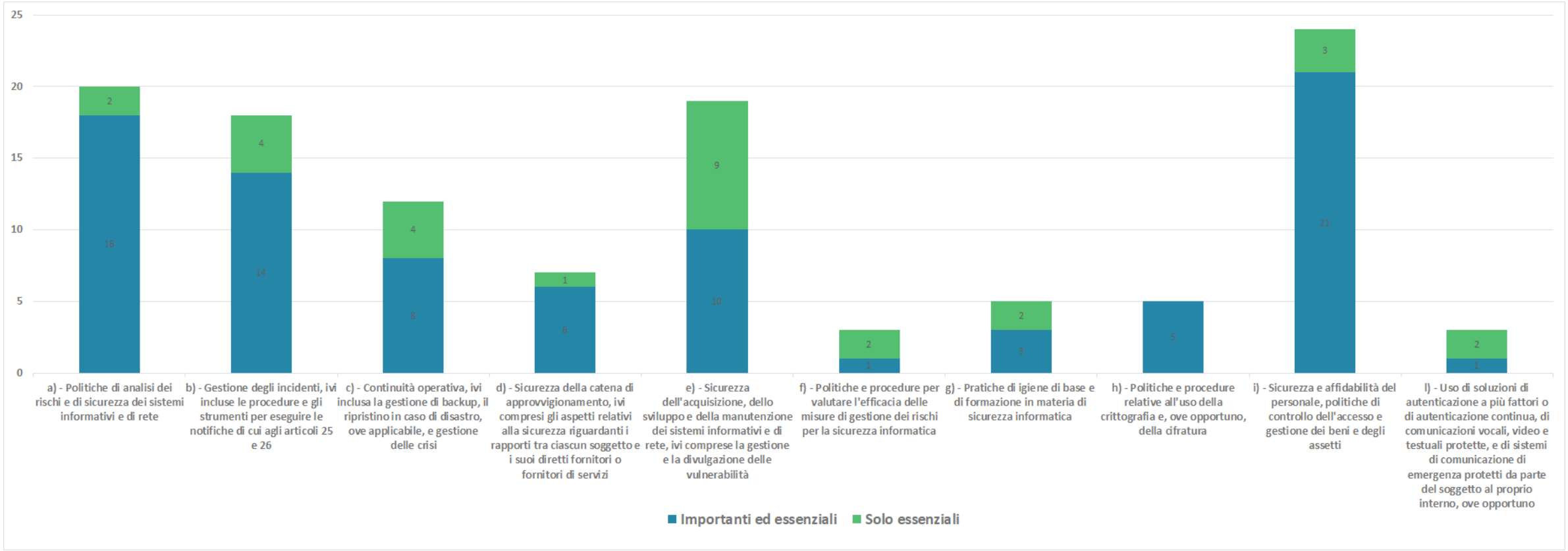
Misure di sicurezza

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



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.

Tipologia requisiti

Organizzativi

Ad esempio:

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

Tecnologici

Ad esempio:

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

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

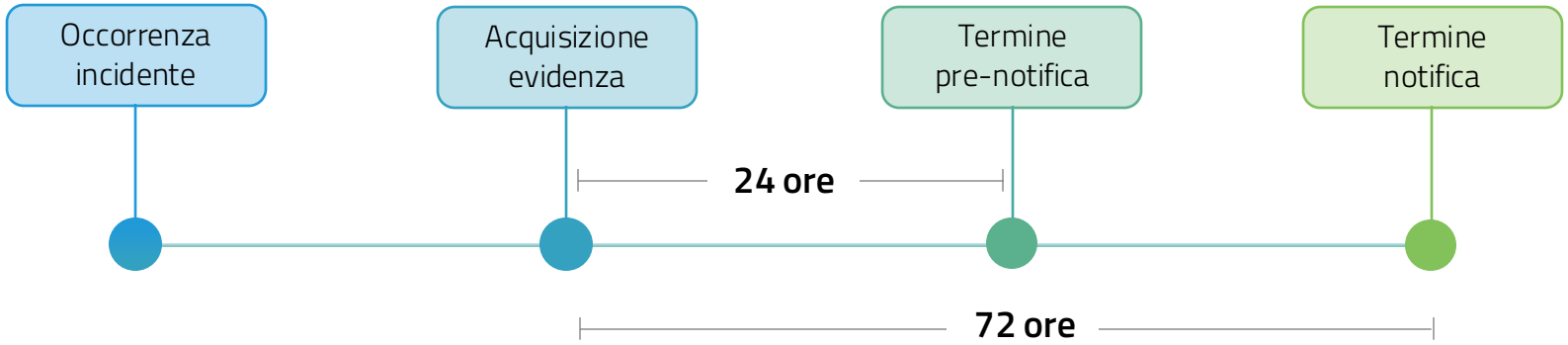
Solo soggetti essenziali
1 tipologia di incidente

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..

Misure di sicurezza

Sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza dei rapporti con i diretti fornitori o i fornitori di servizi .

Ambiti di applicazione delle misure di sicurezza

Politiche di analisi dei rischi e di sicurezza dei sistemi informativi

Gestione degli incidenti

Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi

Sicurezza catena di approvvigionamento, compresi aspetti relativi sicurezza rapporti con diretti fornitori o fornitori di servizi

Sicurezza acquisizione, sviluppo e manutenzione dei sistemi informativi e di rete, ivi compresa gestione e divulgazione vulnerabilità

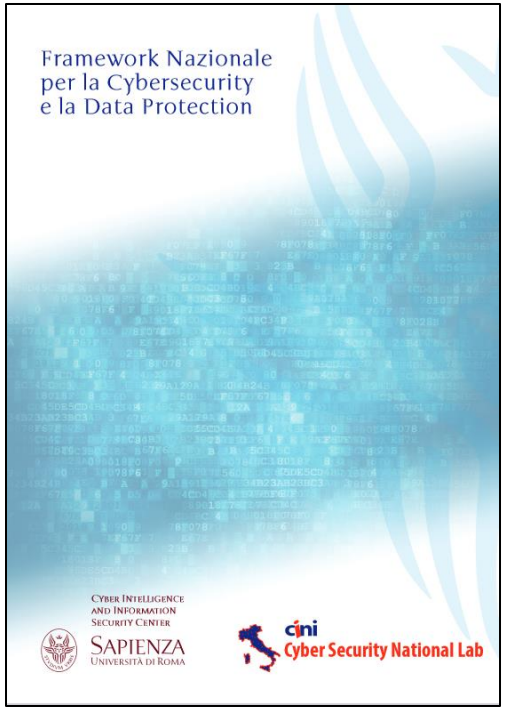
Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza

Pratiche di igiene informatica di base e formazione in materia di cybersicurezza

Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura

Sicurezza risorse umane, strategie di controllo dell'accesso e gestione degli assetti

Uso di soluzioni di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti



Processo per la sicurezza della Supply Chain

FASE 1

GV.SC-07 punto 1
Valutazione del rischio associato alla fornitura.

FASE 2

GV.SC-01
Definizione requisiti di sicurezza sulla fornitura.

FASE 3

GV.SC-05
Inserimento requisiti in bandi di gara, contratti, accordi, etc.

FASE 4

GV.SC-07 punto 2
Verifica conformità della fornitura ai requisiti.

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

Principi generali

5 Misure di sicurezza per la Supply Chain

- ✓ Basate su nuova versione Framework Nazionale per la Cybersecurity e la Data Protection (edizione 2025).
- ✓ Ogni misura costituita da; codice + descrizione + requisiti.
- ✓ 7 requisiti per entrambi tipologie soggetti, 1 requisito per i soli soggetti essenziali.

Approccio basato sul rischio

- ✓ Forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete (eventuale compromissione della fornitura può determinare effetti sulla sicurezza dei sistemi informativi e di rete).
- ✓ Il rischio associato alla fornitura determina i requisiti di sicurezza.

Esempio

GV.SC-07 ← Codice identificativo

I rischi posti da un fornitore, dai suoi prodotti e servizi e da altre terze parti sono compresi, registrati, prioritizzati, valutati, trattati e monitorati nel corso della relazione. ← Descrizione misura

PUNTO	REQUISITO	S_I	S_E
1	Nell'ambito della valutazione del rischio di cui alla misura ID.RA-05, è valutato e documentato il rischio associato alle forniture. A tal fine, sono valutati almeno: a) il livello di accesso del fornitore ai sistemi informativi e di rete del soggetto NIS; b) l'accesso del fornitore alla proprietà intellettuale e ai dati anche sulla base della loro criticità; c) l'impatto di una grave interruzione della fornitura; d) i tempi e i costi di ripristino in caso di indisponibilità dei servizi; e) i ruoli e le responsabilità del fornitore nel governo dei sistemi informativi e di rete.	●	●
2	È verificata periodicamente e documentata la conformità delle forniture ai requisiti di cui alla misura GV.SC-05.	●	●

Specifiche requisiti

Misure di sicurezza (1/2)

Requisiti di 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.

- Forniture con potenziali impatti sulla la sicurezza dei sistemi informativi e di rete.
- Coinvolgimento organizzazione di cybersecurity.
- Requisiti in accordo al rischio associato alla fornitura.
- Coerenza con misure applicate dal soggetto.
- Indicati ambiti minimi dei requisiti per i soggetti essenziali.

Ruoli e responsabilità

GV.SC-02: I ruoli e le responsabilità in materia di cybersecurity per fornitori, clienti e partner sono stabiliti, comunicati e coordinati internamente ed esternamente.

- Definizione ruoli e responsabilità in materia di sicurezza informatica assegnati a eventuali terze parti.
- Comunicazione alle articolazioni competenti del soggetto.

Misure di sicurezza (2/2)

Censimento fornitori

GV.SC-04: I fornitori sono noti e prioritizzati in base alla criticità.

- Inventario di fornitori e partner terzi.
- Indicazione punti di contatto e tipologia fornitura.

Bandi di gara e contratti

GV.SC-05: I requisiti per affrontare i rischi di cybersecurity nella catena di approvvigionamento sono stabiliti, prioritizzati e integrati nei contratti e in altri tipi di accordi con i fornitori e altre terze parti rilevanti.

- Inserimento requisiti di sicurezza in richieste di offerta, bandi di gara e contratti relative a forniture rilevanti.
- Fatte salve motivate e documentate ragioni.

Valutazione rischio e verifica conformità

GV.SC-07: I rischi posti da un fornitore, dai suoi prodotti e servizi e da altre terze parti sono compresi, registrati, prioritizzati, valutati, trattati e monitorati nel corso della relazione.

- Indicati elementi per valutazione rischio associato alle forniture.
- Verifica periodica della conformità delle forniture.

Decreto Legislativo NIS

Proporzionalità e gradualità

Gradualità degli obblighi

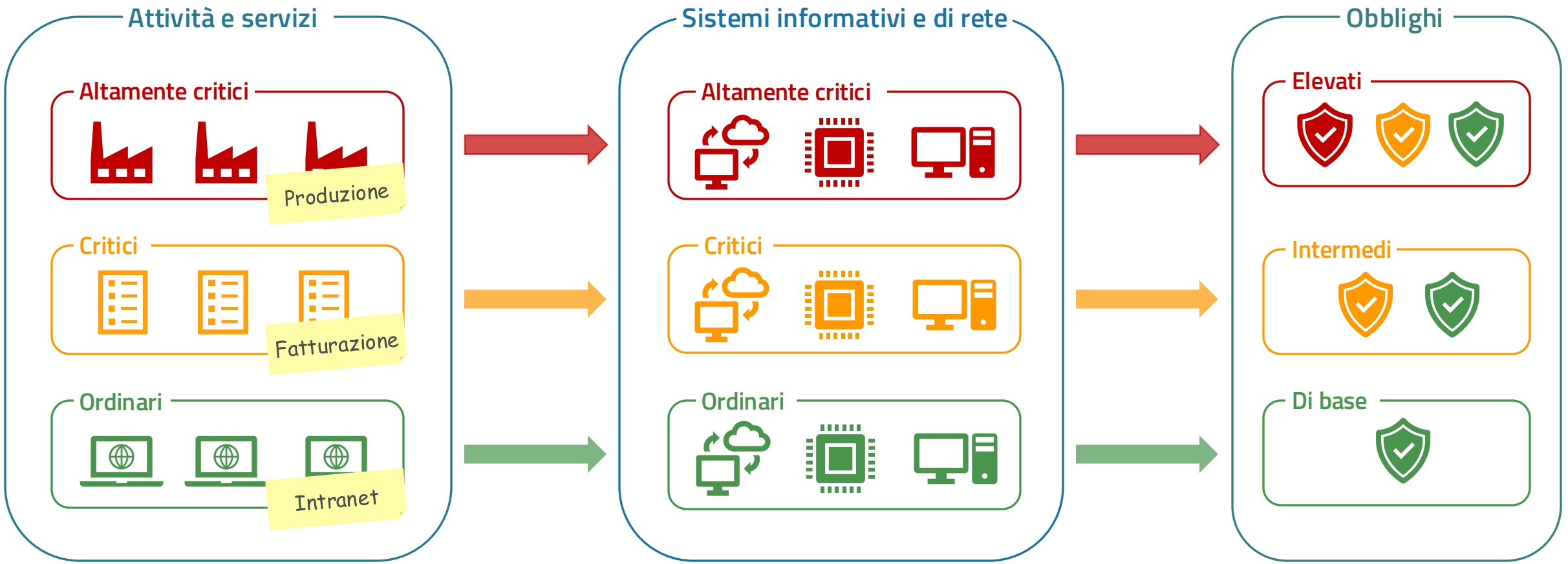
Specifiche di base

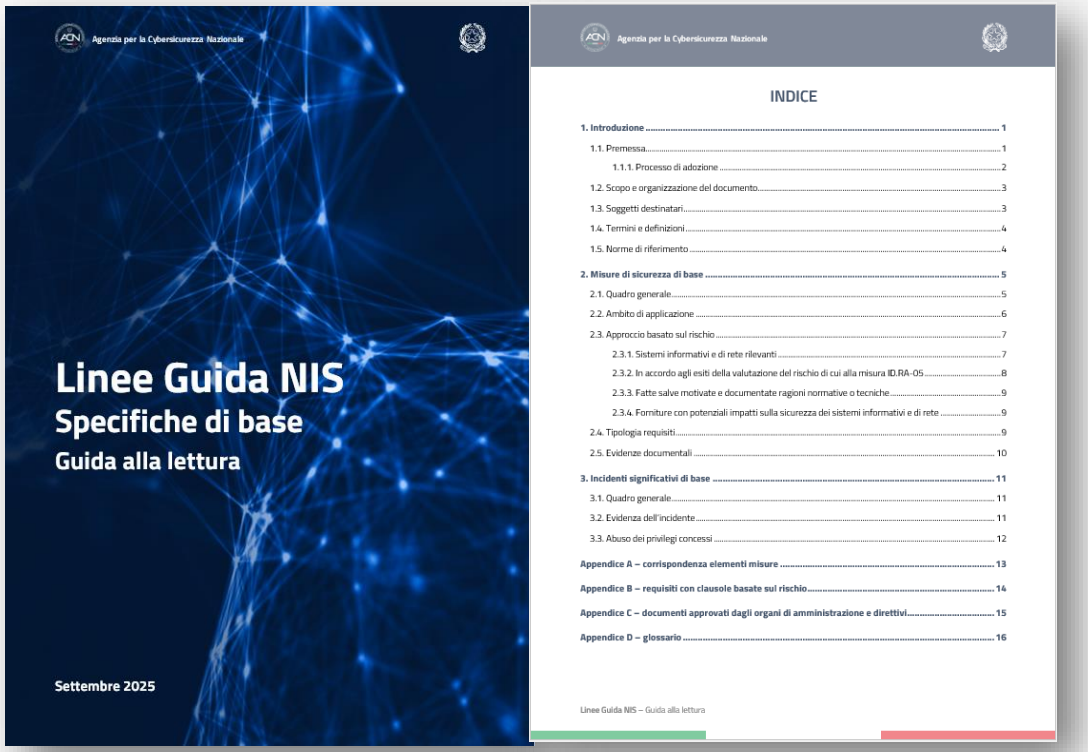
Specifiche degli obblighi, anche orizzontali, minimi per tutta l'infrastruttura con un orizzonte a breve termine.

Specifiche a lungo termine

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

Proporzionalità degli obblighi





Linee Guida NIS – Specifiche di base – Guida alla lettura

Appendici

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.

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.

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.

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

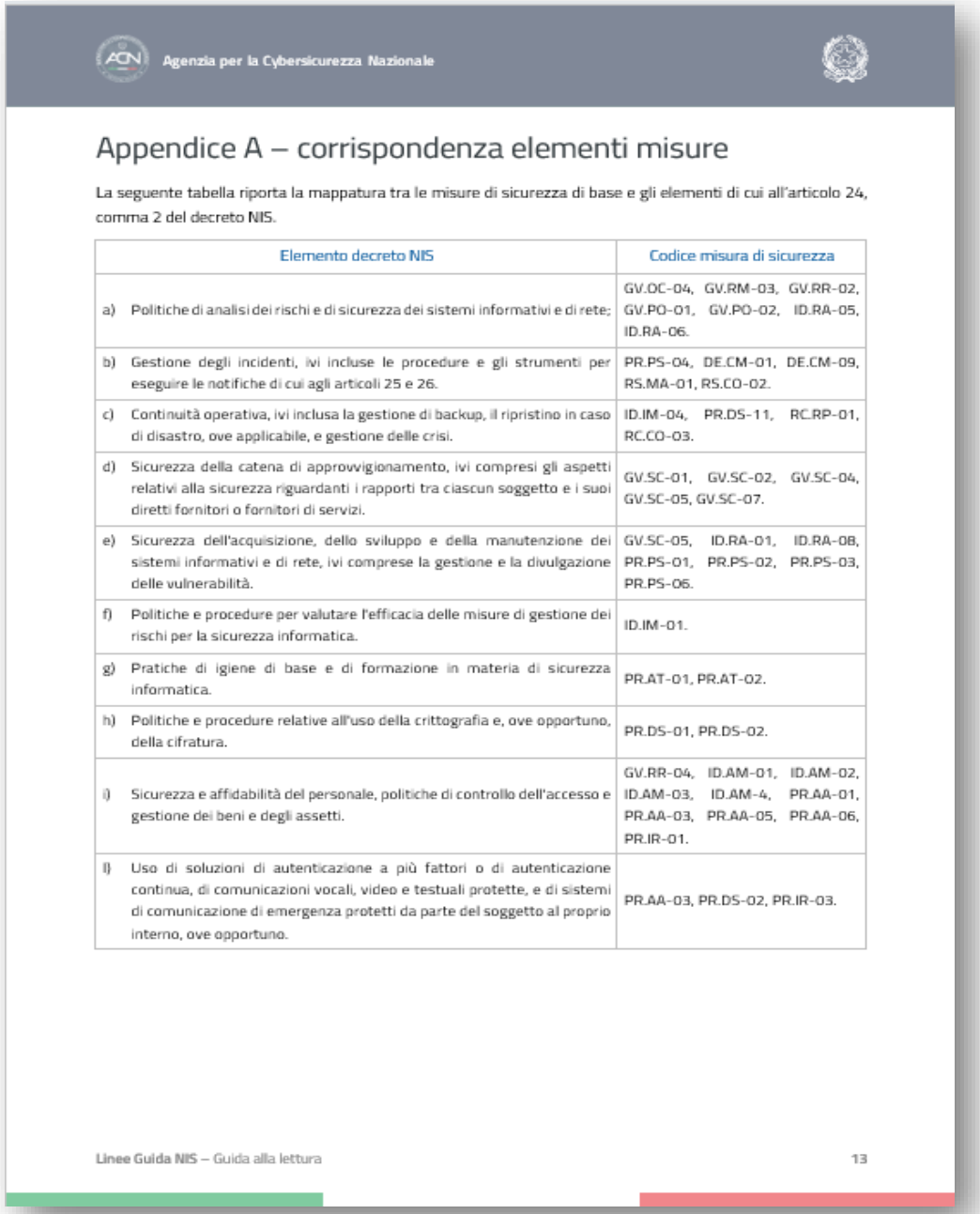
Il decreto legislativo 4 settembre 2024, n. 138.

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

Appendici 1/4

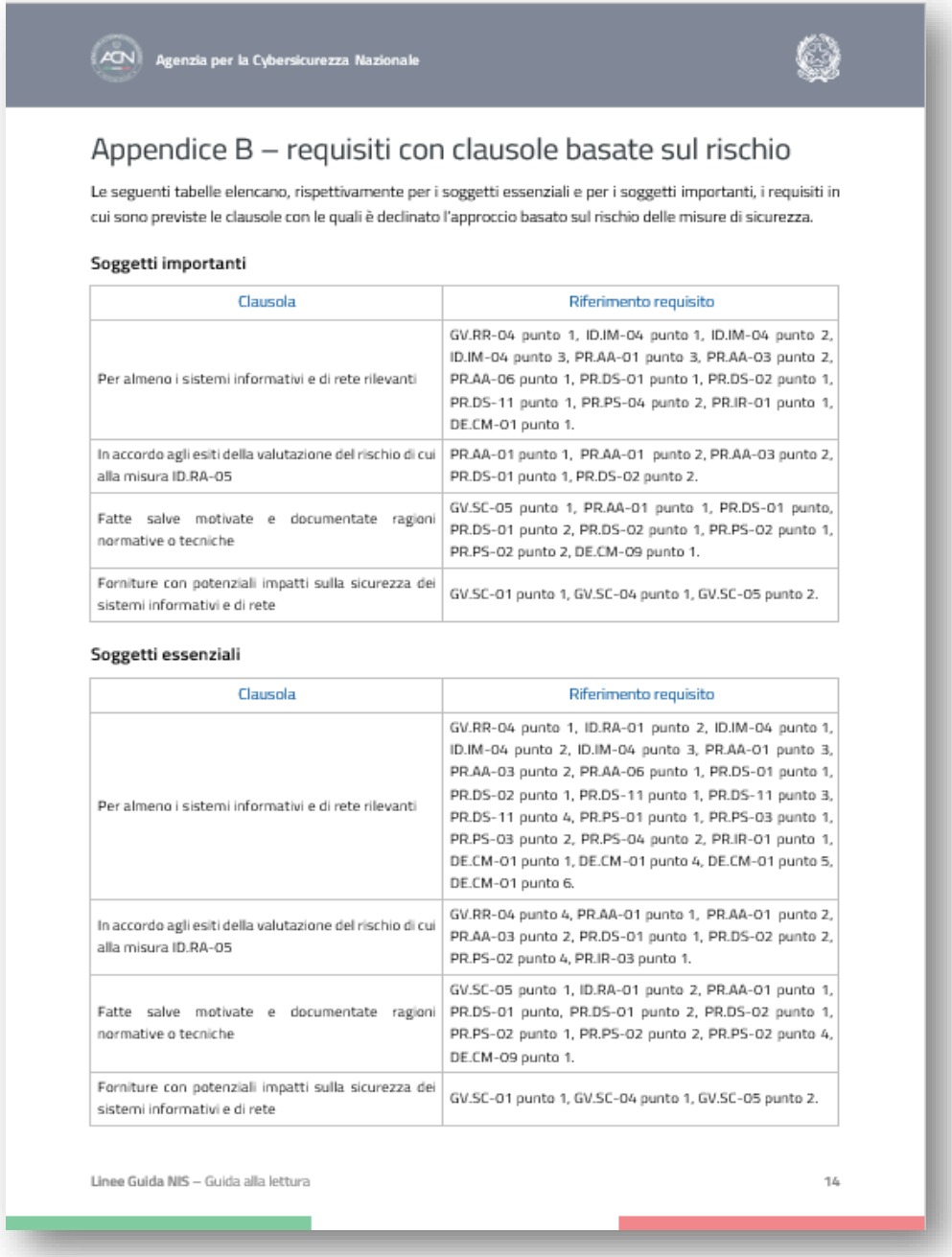


Appendice A – corrispondenza elementi misure

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.

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.

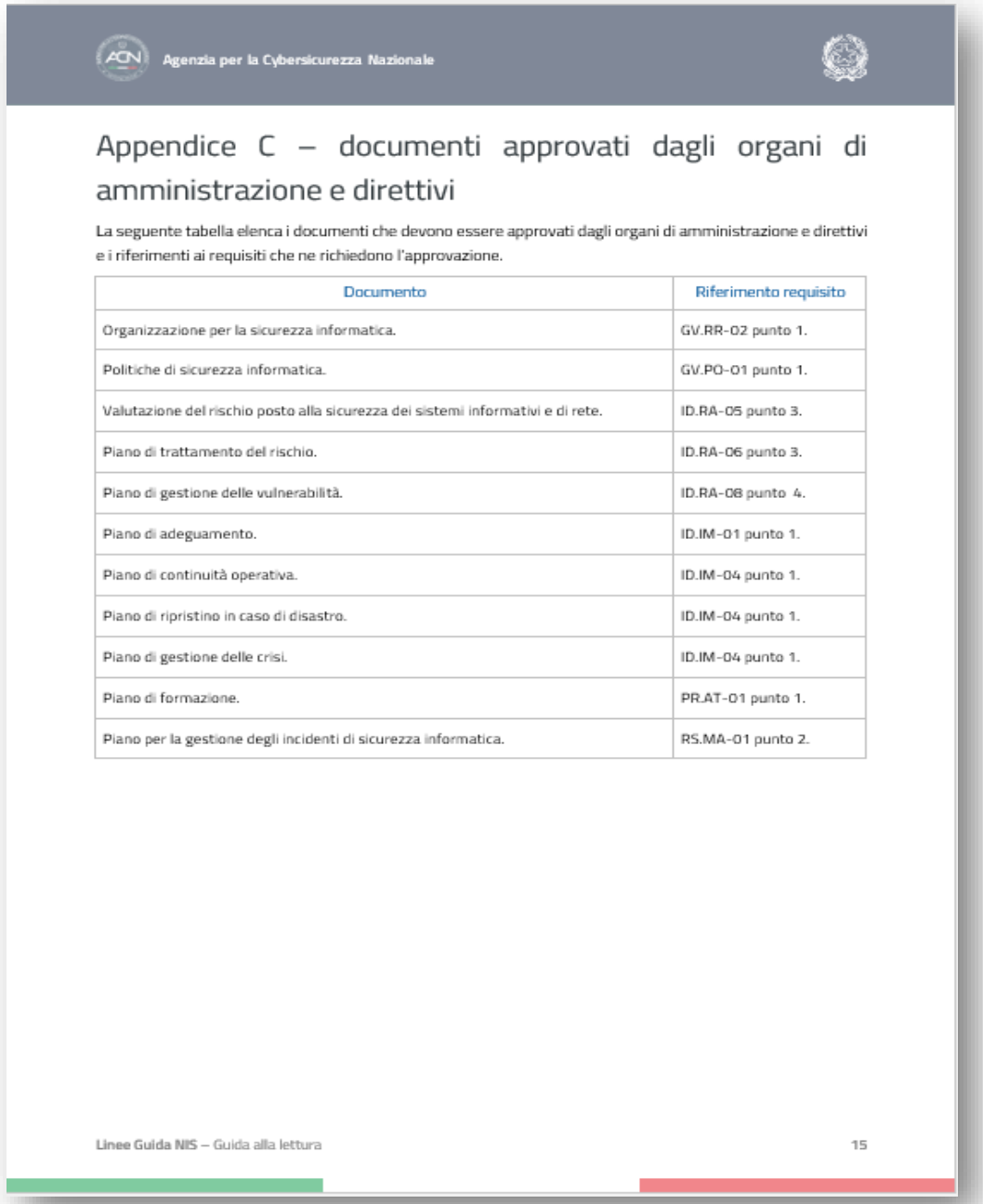
Soggetti importanti

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

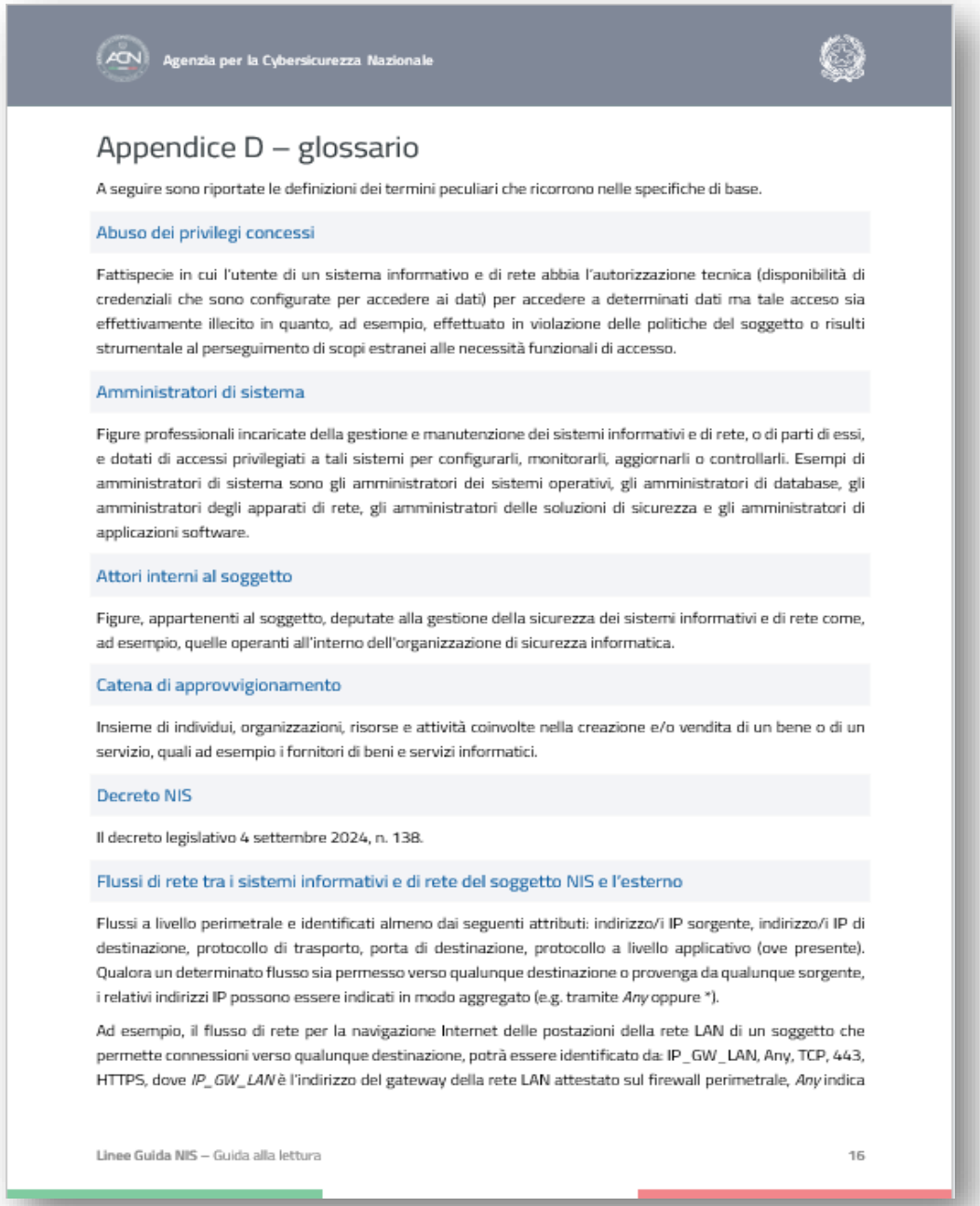


Appendice C – documenti approvati dagli organi di amministrazione e direttivi

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



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

Prossimi passi

Scadenze

Conferma del link da parte dei componenti degli organi di amministrazione e direttivi
- 31 ottobre 2025

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/