Nuova disciplina NIS

Specifiche di base: misure di sicurezza e incidenti.

18 maggio 2025

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

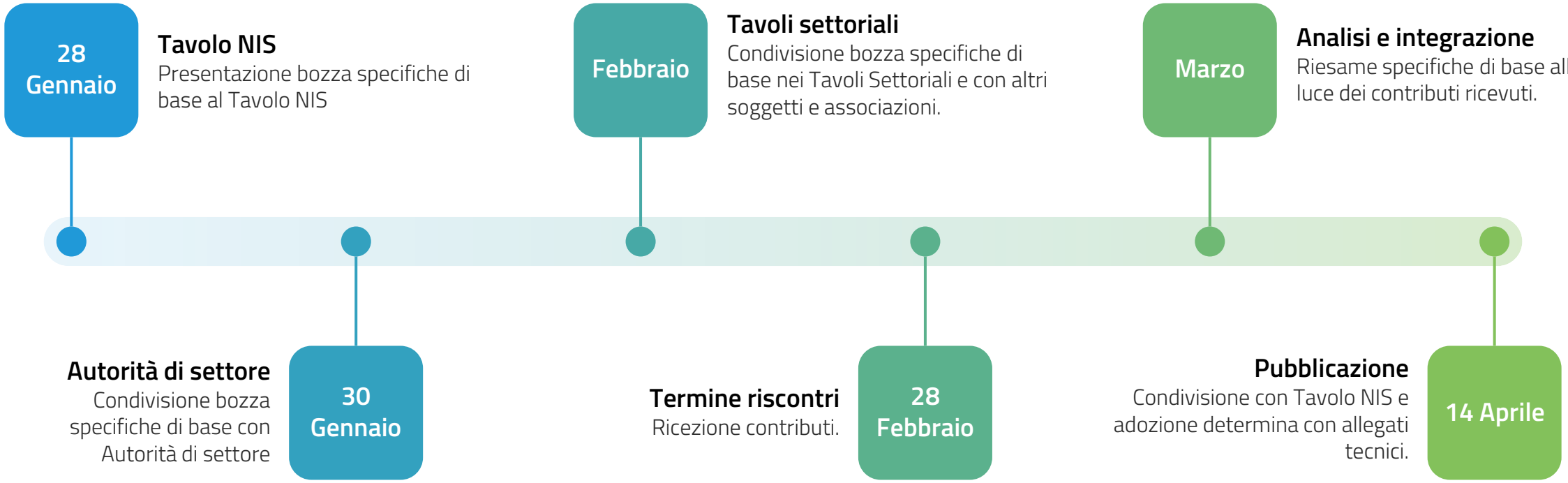
Allegato 1
Misure di sicurezza di base soggetti importanti

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



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)

Processo di sviluppo

Framework Core

Funzioni	Categorie	Sottocategorie	Informative References
GOVERNO (GV)			
IDENTIFICAZIONE (ID)			
PROTEZIONE (PR)			
RILEVAMENTO (DE)			
RISPOSTA (RS)			
RIPRISTINO (RC)			

Framework contestualizzato

Funzioni	Categorie	Sottocategorie	Informative References
GOVERNO (GV)			
IDENTIFICAZIONE (ID)			
PROTEZIONE (PR)			
RILEVAMENTO (DE)			
RISPOSTA (RS)			
RIPRISTINO (RC)			

43 sottocategorie

Misure di sicurezza

ALLEGATO 2

Misure di sicurezza di base per i soggetti essenziali

1. GOVERNO (GOVERN)

1.1. **Contesto organizzativo (GV.OC)**: Il contesto – missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali – che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso[1].

1.1.1. **GV.OC-4**: Gli obiettivi, le capacità e i servizi critici dai quali gli stakeholder dipendono o che si aspettano dall'organizzazione sono compresi e comunicati.

1. È mantenuto un elenco aggiornato dei sistemi informativi e di rete rilevanti.

1.2. **Strategia di gestione del rischio (GV.RM)**: Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo.

1.2.1. **GV.RM-03**: Le attività e gli esiti della gestione del rischio di cybersecurity sono parte integrante dei processi di gestione del rischio dell'organizzazione.

1. Nell'ambito dei processi di gestione del rischio del soggetto NIS e nel rispetto delle politiche di cui alla misura GV.PO-01, è definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica per identificare, analizzare, valutare, trattare e monitorare i rischi.

116 requisiti

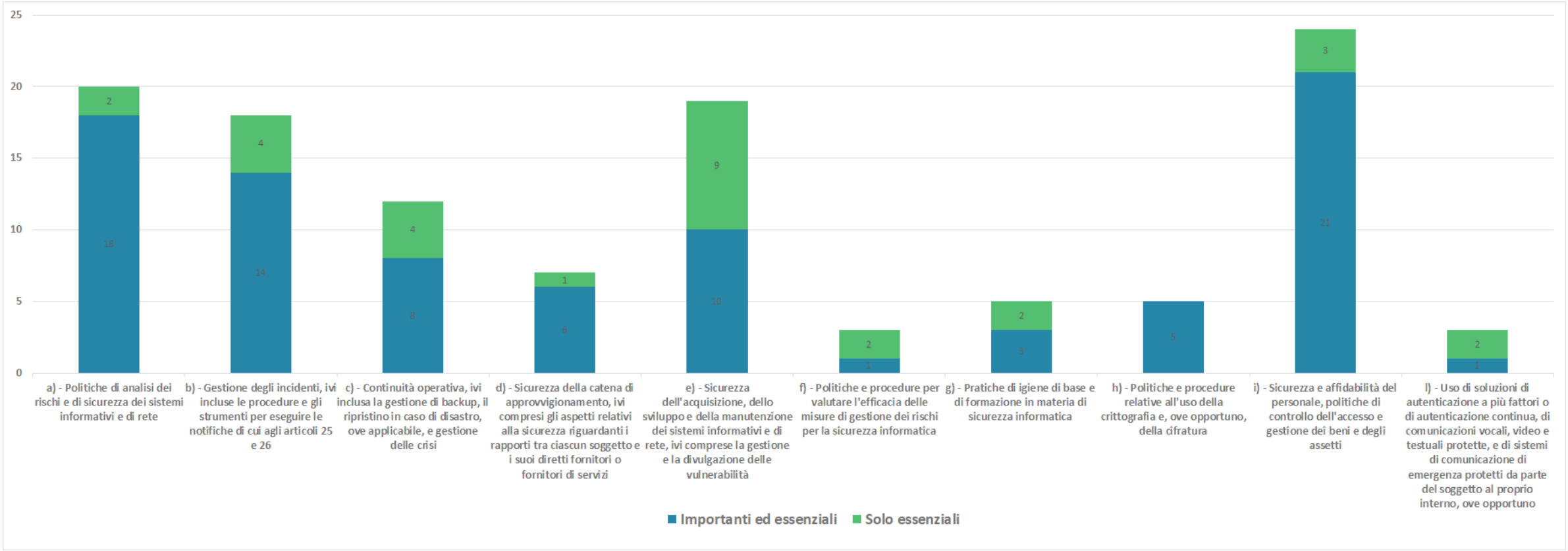
Selezione sottocategorie

Definizione requisiti

Previsioni D.Lgs. 138/2024

Best practice

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



Approccio basato sul rischio

Ambito	Livello di rischio	Proporzionalità	Approccio	Clausole
Le misure di sicurezza si applicano a tutti i sistemi informativi e di rete del soggetto.	Ogni sistema informativo e di rete è caratterizzato da un proprio livello di rischio.	L'art. 31 del decreto prevede che si tenga conto, nello stabilire gli obblighi, del grado di esposizione dei soggetti ai rischi.	Le misure di sicurezza sono state sviluppate secondo un approccio basato sul rischio.	Previsione per i requisiti di maggiore complessità di specifiche clausole.

Declinazione approccio basato sul rischio

13 requisiti per i soggetti importanti e **22** per i soggetti essenziali

5 requisiti per i soggetti importanti e **8** 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

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.

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*.

Politiche di sicurezza informatica

1.4.1. **GV.PO-01**: La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.

1. Sono adottate e documentate politiche di sicurezza informatica per almeno i seguenti ambiti:
   a) gestione del rischio;
   b) ruoli e responsabilità;
   c) affidabilità delle risorse umane;
   d) conformità e audit di sicurezza;
   e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;
   f) gestione degli asset;
   g) gestione delle vulnerabilità;
   h) continuità operativa, ripristino in caso di disastro e gestione delle crisi;
   i) gestione dell'autenticazione, delle identità digitali e del controllo accessi;
   j) sicurezza fisica;
   k) formazione del personale e consapevolezza;
   l) sicurezza dei dati;
   m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
   n) protezione delle reti e delle comunicazioni;
   o) monitoraggio degli eventi di sicurezza;
   p) risposta agli incidenti e ripristino.
2. Per gli ambiti di cui al punto 1 sono incluse almeno le politiche in relazione ai requisiti indicati nella tabella 1 in appendice al presente allegato.
3. Le politiche di cui al punto 1 sono approvate dagli organi di amministrazione e direttivi.

3.3.3. **PR.DS-11**: I backup dei dati sono creati, protetti, mantenuti e verificati.

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.

Tabella 1: Requisiti di cui al punto 2 della misura GV.PO-01.

Ambiti Politiche	Requisiti
a) Gestione del rischio.	GV.OC-04: punto 1. GV.RM-03: punto 1. ID.RA-05: punti 1, 2 e 3. ID.RA-06: punti 1, 2 e 3.
b) Ruoli e responsabilità.	GV.RR-02: punti 1, 2, 3 e 4.
c) Affidabilità delle risorse umane.	GV.RR-04: punti 1 e 2.
d) Conformità e audit di sicurezza.	GV.PO-01: punti 1, 2 e 3. GV.PO-02: punti 1 e 2. ID.IM-01: punti 1 e 2.
e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento.	GV.SC-01: punto 1. GV.SC-02: punto 1. GV.SC-04: punto 1. GV.SC-05: punto 1. GV.SC-07: punti 1 e 2.
f) Gestione degli asset.	ID.AM-01: punto 1. ID.AM-02: punto 1. ID.AM-04: punto 1.
g) Gestione delle vulnerabilità.	ID.RA-01: punto 1. ID.RA-08: punti 1, 2, 3 e 4.
h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi.	ID.IM-04: punti 1, 2, 3, 4 e 5.
i) Gestione dell'autenticazione, delle identità digitali e del controllo accessi.	PR.AA-01: punti 1, 2 e 3. PR.AA-03: punti 1 e 2. PR.AA-05: punti 1 e 2. PR.IR-01: punti 1 e 2.
j) Sicurezza fisica	PR.AA-06: punto 1.
k) Formazione del personale e consapevolezza.	PR.AT-01: punti 1, 2 e 3.
l) Sicurezza dei dati.	PR.DS-01: punti 1 e 2. PR.DS-02: punto 1. PR.DS-11: punto 1.
m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete.	PR.PS-02: punti 1, 2. PR.PS-04: punti 1, 2 e 3. PR.PS-06: punto 1.
n) Protezione delle reti e delle comunicazioni.	PR.IR-01: punto 3.
o) Monitoraggio degli eventi di sicurezza.	DE.CM-01: punti 1 e 2. DE.CM-09: punto 1.
p) Risposta agli incidenti e ripristino.	RS.MA-01: punti 1, 2 e 3. RS.CO-02: punti 1 e 2. RC.RP-01: punto 1.

Processo di sicurezza per la 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

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

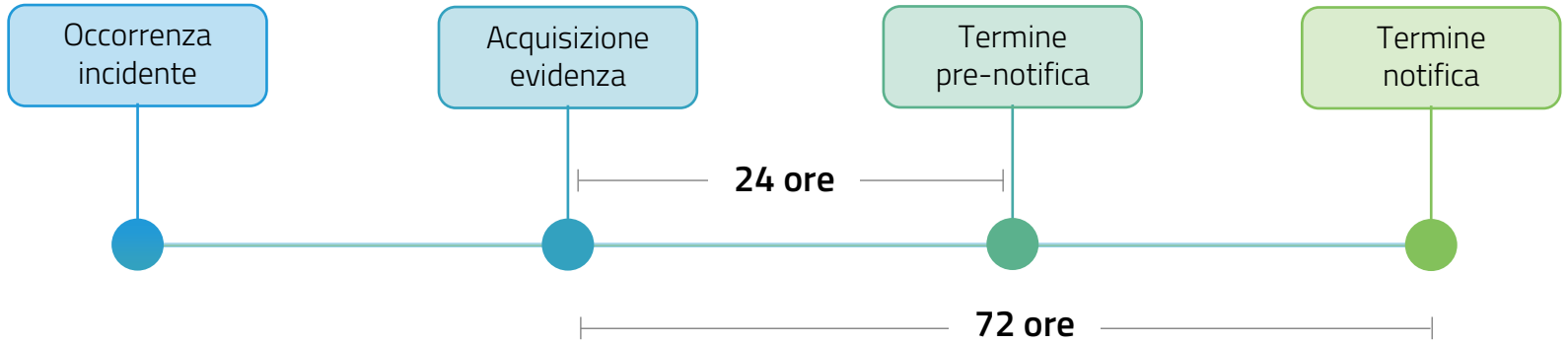
Solo soggetti essenziali
1 tipologia di incidente

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..

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/