M4 S.p.A.

PROCEDURA SU CYBER SECURITY MANAGEMENT POLICY M4

STATO DEL DOCUMENTO	Emesso da:	Verificato da:
Identificazione: Cyber Security Management Policy M4	Construction Manager	Presidente
	[firma] 	[firma] 
Approvata dal Consiglio di Amministrazione in data 08/10/2026		

Lista delle modifiche			
Identificazione	**Revisione**	**Data**	**Tipo di modifica**
Cyber Security Management Policy M4	00	30/09/2026	Prima emissione

INDICE

1 Ambito e Obiettivi

2 Principali destinatari

3 Perimetro di applicabilità

4 Principi di riferimento

5 Riferimenti

6 Definizioni e abbreviazioni

7 Organizzazione della sicurezza informatica di M4

8 Sistema di gestione e architettura documentale

9 Ambiti di sicurezza: principi e processi indirizzati

10 Informativa agli organi di amministrazione

11 Eccezioni e violazioni

12 Aggiornamento e gestione della documentazione

13 Allegati

1 - Ambito e Obiettivi

M4 S.p.A. (di seguito anche «M4» o «la Società»), titolare della Linea 4 della metropolitana di Milano, è qualificata come **soggetto essenziale** ai sensi del D.Lgs. 138/2024 (di seguito «Decreto NIS2»), di recepimento della Direttiva (UE) 2022/2555 («Direttiva NIS2»).

Il presente documento costituisce la **Policy di Sicurezza Informatica unica di M4**, valida per l'intera Società, secondo gli indirizzi presentati al Consiglio di Amministrazione di M4 nella seduta del 10 settembre 2026. M4 adotta un **unico documento di sintesi** che:

- esprime l'organizzazione della sicurezza informatica di M4: i ruoli istituiti ai sensi del Decreto NIS2 e il riparto delle responsabilità tra gli organi e le funzioni di M4, il Gestore del Servizio (ATM S.p.A.) e i fornitori (misura GV.RR-02);
- fissa i principi e gli indirizzi per ciascuno dei sedici ambiti che le politiche di sicurezza devono disciplinare ai sensi della misura GV.PO-01;
- indirizza il dettaglio operativo di ciascun ambito verso i **processi** che lo attuano e verso i **piani** approvati dal Consiglio di Amministrazione ai sensi dell'art. 23 del Decreto NIS2, la cui documentazione è conservata nel repository documentale NIS2 di M4.

La Policy persegue i seguenti obiettivi:

- garantire la riservatezza, l'integrità e la disponibilità dei sistemi informativi e di rete di M4 e, per il loro tramite, la continuità e la sicurezza dell'esercizio della Linea 4;
- assicurare la conformità agli obblighi del Decreto NIS2, con particolare riferimento agli artt. 23 (organi di amministrazione e direttivi), 24 (misure di gestione dei rischi) e 25 (notifica degli incidenti significativi), e alle Determinazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN);
- rendere esplicito che la responsabilità per gli obblighi del Decreto NIS2 resta in capo a M4 e ai suoi organi di amministrazione anche per le attività affidate in gestione ad ATM S.p.A. o a fornitori, e stabilire i meccanismi con cui M4 esercita tale responsabilità;
- fornire al Consiglio di Amministrazione gli elementi per approvare le modalità di implementazione delle misure e sovrintenderne l'attuazione;
- costituire il riferimento unico da cui discendono i processi, i piani, i registri e gli inventari del perimetro di M4.

Restano al di fuori dell'ambito della presente Policy la sicurezza dell'esercizio ferroviario (safety), disciplinata dalla normativa di settore e presidiata da ANSFISA, la sicurezza sul luogo di lavoro e la protezione dei beni non afferenti ai sistemi informativi e di rete, salvo per i profili in cui tali ambiti interagiscono con la sicurezza informatica.

2 - Principali destinatari

La presente Policy è destinata a:

- i componenti del Consiglio di Amministrazione e gli organi direttivi di M4;
- il Rappresentante Legale, il Punto di Contatto NIS2 e il suo sostituto;
- il personale di M4 e le funzioni aziendali di M4, per gli ambiti di rispettiva competenza;
- ATM S.p.A., in qualità di Gestore del Servizio e fornitore di M4, per le attività svolte sul perimetro di M4, per il tramite del Contratto di gestione;
- i fornitori, i manutentori, i consulenti e le altre terze parti che accedono ai sistemi informativi e di rete di M4 o ne gestiscono componenti, per il tramite dei rispettivi contratti.

3 - Perimetro di applicabilità

3.1 Perimetro soggettivo

La Policy si applica a M4. Si applica inoltre al Gestore del Servizio e ai fornitori nella misura in cui operano sui sistemi informativi e di rete del perimetro di M4: per tali soggetti i requisiti della Policy si ritrovano nel Contratto di gestione, opportunamente aggiornato per essere in linea con le nuove necessità introdotte dall'evoluzione del contesto di rischio e con le normative quali il decreto NIS2, e i contratti di fornitura, che devono recepirli (cfr. §8.1 e §9.5).

3.2. Perimetro oggettivo: i due domini

La Policy si applica ai sistemi informativi e di rete di M4 rilevanti per la prestazione delle attività e dei servizi comunicati all'ACN ai sensi dell'art. 30 del Decreto NIS2. Il perimetro si articola in due domini, che differiscono per modello di gestione e non per livello di protezione richiesto: il dominio OT di linea, prevalente, affidato in gestione al Gestore del Servizio, e il dominio IT corporate, residuale, gestito direttamente da M4.

Dominio	Contenuto	Titolarità	Gestione operativa	Disciplina di dettaglio
Dominio OT di linea	Reti di esercizio e di stazione, sistemi tecnologici di impianto a supporto dell'esercizio automatico della linea, server farm OT, interconnessioni con reti esterne, con il Gestore e con fornitori e manutentori	M4, quale Titolare del Servizio	ATM S.p.A., quale Gestore del Servizio, in forza del Contratto di gestione; fornitori e manutentori di impianto	Processi del Gestore, documentati nel repository NIS2 di M4
Dominio IT corporate	Postazioni di lavoro, applicazioni, servizi di posta e collaborazione, servizi cloud e SaaS, reti degli uffici di M4	M4	Funzione IT di M4 e fornitori IT di M4 (non ricompreso nel Contratto di gestione)	Processi di M4 e dei fornitori IT, documentati nel repository NIS2 di M4

Tabella 1 – Domini del perimetro di M4

Per ciascun ambito di sicurezza la presente Policy indirizza un processo, che è eseguito dal soggetto che gestisce il dominio interessato secondo requisiti omogenei per entrambi i domini (cfr. §8.3 e Allegato 1).

4 - Principi di riferimento

Il sistema di gestione della sicurezza informatica di M4 si fonda sui seguenti principi, che vincolano la redazione e l'applicazione di tutti i documenti che discendono dalla presente Policy.

- **Riservatezza, integrità e disponibilità.** Le informazioni e i sistemi sono accessibili solo a chi è autorizzato, restano accurati e completi e sono utilizzabili quando richiesto. Nel dominio OT di linea la disponibilità e l'integrità dei sistemi che abilitano l'esercizio hanno priorità, e ogni misura di sicurezza deve essere valutata anche rispetto ai suoi effetti sulla continuità e sulla sicurezza dell'esercizio.
- **La gestione si affida, la responsabilità resta.** L'affidamento al Gestore del Servizio o a fornitori dell'esecuzione di attività di sicurezza non trasferisce la responsabilità degli obblighi del Decreto NIS2, che resta in capo a M4 e ai suoi organi di amministrazione. M4 esercita tale responsabilità attraverso requisiti contrattuali, flussi informativi, autorizzazione delle modifiche e diritto di verifica.
- **Approccio basato sul rischio e proporzionalità.** Le misure sono commisurate al rischio, allo stato dell'arte, ai costi di attuazione e alla gravità dei possibili incidenti, come previsto dall'art. 24 del Decreto NIS2.
- **Una policy, processi indirizzati.** La presente Policy stabilisce che cosa deve essere garantito e indirizza i processi che lo attuano; la documentazione dei processi, predisposta dai soggetti che li eseguono, stabilisce come, da chi e con quale frequenza. Tale documentazione non può derogare ai requisiti della Policy né indebolirne i parametri.

- **Prescrittività.** La documentazione dei processi descrive come si deve operare, non lo stato di fatto. Il divario tra requisito e situazione attuale non riduce il requisito: è registrato tra le azioni di adeguamento del processo e alimenta il piano di adeguamento (misura ID.IM-01) e il registro dei rischi.
- **Equivalenza con i processi del Gestore.** Il Gestore del Servizio può attuare i requisiti del perimetro di M4 mediante i propri processi e strumenti, a condizione che assicurino un livello di protezione almeno equivalente a quello richiesto dalla presente Policy e che le evidenze siano rese disponibili a M4. In caso di divergenza prevale il requisito più stringente.
- **Evidenza.** Ogni requisito deve produrre evidenze verificabili, conservate e disponibili a M4, agli organi di controllo e all'ACN.
- **Tracciabilità delle modifiche.** Nessuna modifica all'infrastruttura del dominio OT di linea è eseguita senza la preventiva autorizzazione di M4, secondo quanto previsto dal Contratto di gestione.
- **Miglioramento continuo.** Il sistema è gestito secondo il ciclo Plan-Do-Check-Act ed è riesaminato almeno annualmente (cfr. §12.1).

5- Riferimenti

5.1 Riferimenti normativi esterni

- Direttiva (UE) 2022/2555 (c.d. Direttiva NIS2) e D.Lgs. 4 settembre 2024, n. 138 di recepimento, con particolare riferimento agli artt. 7 (registrazione), 23 (organi di amministrazione e direttivi), 24 (misure di gestione dei rischi), 25 (notifica degli incidenti significativi), 30 (elencazione delle attività e dei servizi), 37 e 38 (regime sanzionatorio);
- Determinazioni del Direttore Generale dell'ACN adottate in attuazione del D.Lgs. 138/2024 (fonte: acn.gov.it/portale/nis/la-normativa), riportate nell'Allegato 2;
- Direttiva (UE) 2022/2557 (c.d. Direttiva CER) e D.Lgs. 4 settembre 2024, n. 134, sulla resilienza dei soggetti critici;
- Regolamento (UE) 2016/679 (GDPR) e D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. 10 agosto 2018, n. 101;
- D.Lgs. 8 giugno 2001, n. 231, sulla responsabilità amministrativa degli enti;
- Regolamento (UE) 2024/2847 (c.d. Cyber Resilience Act), per i requisiti di sicurezza dei prodotti con elementi digitali acquisiti da M4;
- art. 12 del D.L. 28 settembre 2018, n. 109, convertito dalla L. 16 novembre 2018, n. 130, istitutivo di ANSFISA.

5.2 Riferimenti contrattuali

- Convenzione Unica tra M4 e il Concedente, che disciplina la concessione della Linea 4;
- Contratto di gestione (O&M) tra M4, quale Titolare del Servizio, e ATM S.p.A., quale Gestore del Servizio;
- contratti con i fornitori e i manutentori dei sistemi informativi e di rete di M4.

5.3 Riferimenti interni

- informative e delibere del Consiglio di Amministrazione di M4 del 18/12/2025, 27/04/2026, 15/06/2026 e 10/09/2026 in materia NIS2;
- atti di nomina del Punto di Contatto NIS2 e di designazione del Referente CSIRT e dei sostituti;
- Risk Assessment e piani approvati dal Consiglio di Amministrazione ai sensi dell'art. 23 del Decreto NIS2 (cfr. §8.2);
- documentazione di attuazione dei processi indirizzati dalla presente Policy (piani, procedure, registri ed evidenze), conservata nel repository documentale NIS2 di M4;
- Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 di M4.

5.4 Standard e best practice

- ISO/IEC 27001:2022 e ISO/IEC 27002:2022 – sistemi di gestione della sicurezza delle informazioni e relativi controlli;
- NIST Cybersecurity Framework 2.0, mutuato dall'ACN per la definizione delle misure di sicurezza di base;
- Framework Nazionale per la Cybersecurity e la Data Protection;
- IEC 62443 – sicurezza dei sistemi di automazione e controllo industriale, di riferimento per il dominio OT di linea.

6 - Definizioni e abbreviazioni

Termine	Definizione
ACN	Agenzia per la Cybersicurezza Nazionale, autorità nazionale competente NIS.
CSIRT Italia	Computer Security Incident Response Team nazionale, istituito presso l'ACN, destinatario delle notifiche di incidente ai sensi degli artt. 25 e 26 del Decreto NIS2.
CdA	Consiglio di Amministrazione di M4, organo di amministrazione ai sensi dell'art. 23 del Decreto NIS2.
Concedente	Ente concedente della Linea 4 ai sensi della Convenzione Unica.
Contratto di gestione	Contratto tra M4 e ATM S.p.A. che disciplina l'esercizio del servizio metropolitano della Linea 4 e la gestione delle relative infrastrutture tecnologiche.
Dominio OT di linea	Insieme delle reti, dei sistemi tecnologici di impianto e delle server farm a supporto dell'esercizio della Linea 4, gestito da ATM S.p.A. in forza del Contratto di gestione.
Dominio IT corporate	Insieme dei sistemi informativi e di rete a supporto delle attività aziendali di M4, non ricompreso nel Contratto di gestione.
Eccezione	Deroga motivata, temporanea e approvata a un requisito della presente Policy o della documentazione di un processo, accompagnata da misure compensative e registrata (cfr. §11.1).
Gestore del Servizio	ATM S.p.A., soggetto che gestisce l'esercizio della Linea 4 e le relative infrastrutture tecnologiche in forza del Contratto di gestione.
Incidente significativo	Incidente che soddisfa i criteri dell'art. 25 del Decreto NIS2 e delle Determinazioni ACN, soggetto a notifica al CSIRT Italia.
Misure di base	Misure di sicurezza di base stabilite dalle Determinazioni ACN, articolate secondo le categorie e sottocategorie del NIST CSF 2.0.
Processo indirizzato	Processo con cui è attuato un ambito di sicurezza disciplinato dalla presente Policy; è eseguito dal soggetto che gestisce il dominio interessato e documentato da quest'ultimo.
PdC	Punto di Contatto NIS2 di M4, designato ai sensi del Decreto NIS2 e delle Determinazioni ACN.
Referente CSIRT	Soggetto designato per l'interlocuzione con il CSIRT Italia e per l'effettuazione delle notifiche di cui agli artt. 25 e 26 del Decreto NIS2.
Repository documentale NIS2	Archivio in cui M4 conserva e rende disponibile agli organi, agli organi di controllo e all'ACN la documentazione di attuazione dei processi (piani, procedure, registri ed evidenze), inclusa quella predisposta dal Gestore e dai fornitori.
Sistemi rilevanti	Sistemi informativi e di rete da cui dipende la prestazione delle attività e dei servizi comunicati all'ACN ai sensi dell'art. 30 del Decreto NIS2 (misura GV.OC-04).
SOC	Security Operation Center: servizio di monitoraggio degli eventi di sicurezza operativo 7x24; per il dominio OT di linea è erogato dal Gestore del Servizio.
Titolare del Servizio	M4, titolare dell'infrastruttura tecnologica di esercizio della Linea 4.

Tabella 2 – Definizioni e abbreviazioni

7 - Organizzazione della sicurezza informatica di M4

Il presente capitolo attua la misura GV.RR-02 e definisce l'organizzazione della sicurezza informatica di M4, in coerenza con l'assetto presentato al Consiglio di Amministrazione e con il rapporto tra M4, quale Titolare del Servizio, e ATM S.p.A., quale Gestore del Servizio.

7.1 Il modello in sintesi

L'organizzazione si articola su tre livelli: l'**indirizzo e la supervisione**, esercitati dagli organi di amministrazione; il **governo e il coordinamento**, affidati al Punto di Contatto NIS2; l'**attuazione**, affidata al

Gestore del Servizio per il dominio OT di linea e alle funzioni di M4 e ai fornitori IT per il dominio IT corporate.

Livello	Soggetti	Responsabilità in sintesi
Indirizzo e supervisione	Consiglio di Amministrazione	Approva la Policy, i piani ex art. 23 e il Risk Assessment; sovrintende all'attuazione; è destinatario dell'informativa periodica; risponde delle violazioni ai sensi dell'art. 23 del Decreto NIS2.
Governo e coordinamento	Rappresentante Legale; Punto di Contatto NIS2 e sostituto	Cura il recepimento del Decreto NIS2 e l'implementazione delle misure; governa le linee tecniche e i fornitori, incluso il Gestore per il perimetro di M4; interloquisce con l'ACN; è owner della presente Policy e del framework documentale.
Attuazione – dominio OT di linea	Gestore del Servizio (ATM S.p.A.); fornitori e manutentori di impianto	Attua le misure di sicurezza in forza del Contratto di gestione, monitora gli eventi, gestisce gli incidenti ed esercita il ruolo di Referente CSIRT; rendiconta al PdC.
Attuazione – dominio IT corporate	Funzioni aziendali di M4; fornitori IT di M4	Attua le misure di sicurezza sui sistemi aziendali di M4; segnala gli eventi e gli incidenti; rendiconta al PdC.
Controllo	Collegio Sindacale; Organismo di Vigilanza ex D.Lgs. 231/2001; verificatori indipendenti	Verifica l'adeguatezza e l'effettiva applicazione del sistema, secondo le rispettive competenze.

Tabella 3 – Livelli dell'organizzazione della sicurezza informatica di M4

7.2 Ruoli istituiti ai sensi del Decreto NIS2

Organi di amministrazione e direttivi (CdA). Ai sensi dell'art. 23 del Decreto NIS2:

- approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da M4, e in particolare la presente Policy, i piani ex art. 23 e il Risk Assessment;
- sovrintendono all'implementazione degli obblighi di sicurezza e di notifica degli incidenti, sui quali sono informati su base periodica e, se opportuno, tempestivamente (cfr. cap. 10);
- seguono una formazione specifica in materia di sicurezza informatica e promuovono l'offerta periodica di formazione a tutti i dipendenti;
- sono responsabili delle violazioni degli obblighi discendenti dal Decreto NIS2.

Rappresentante Legale. Delega il Punto di Contatto NIS2 e designa il Referente CSIRT; garantisce la corretta attuazione delle strategie, delle politiche e dei processi aziendali, assicurandone la coerenza con gli obiettivi di business e con i requisiti normativi.

Punto di Contatto NIS2 (PdC). Designato nella persona di M. Di Paola. Il PdC:

- cura e attua il recepimento delle disposizioni del Decreto NIS2, garantendo l'implementazione delle misure di sicurezza;
- raccoglie le informazioni necessarie e comunica e interagisce con l'ACN, curando gli adempimenti ricorrenti sul Portale NIS (registrazione e aggiornamento annuale, elencazione delle attività e dei servizi, elenco dei fornitori rilevanti, aggiornamento dei ruoli entro 14 giorni dalle variazioni);
- governa le linee tecniche e i fornitori, incluso il Gestore del Servizio per le attività sul perimetro di M4;
- è owner della presente Policy, ne cura il riesame e governa il framework documentale che ne discende;
- presiede il Tavolo di coordinamento cyber con il Gestore (cfr. §7.6), predispone l'informativa al CdA e approva le eccezioni nei limiti del §11.1.

Sostituto del Punto di Contatto NIS2. Supporta il PdC e ne assume funzioni e responsabilità in caso di indisponibilità.

Referente CSIRT e sostituti. Con delibera del CdA del 18/12/2025 il ruolo è affidato ad ATM S.p.A., in qualità di Gestore del Servizio, che lo esercita in forza del Contratto di gestione. Il Referente CSIRT interloquisce con il CSIRT Italia ed effettua, in nome e per conto di M4, le notifiche di cui agli artt. 25 e 26 del Decreto NIS2; i sostituti lo supportano o ne svolgono le funzioni. Il Referente CSIRT informa il PdC di ogni notifica contestualmente al suo invio e ne condivide preventivamente i contenuti ogni volta che ciò non comprometta il rispetto dei termini.

7.3 Funzioni aziendali di M4

Le denominazioni delle funzioni che seguono vanno allineate all'organigramma di M4.

- **Funzione tecnica responsabile del Contratto di gestione**: rilascia o nega il nulla osta alle modifiche del dominio OT di linea secondo quanto previsto dal Contratto di gestione, coinvolgendo il PdC quando la modifica presenta impatti sulla sicurezza; verifica l'adempimento degli obblighi di sicurezza del Gestore previsti dal contratto.
- **Funzione IT di M4**: attua le misure di sicurezza sul dominio IT corporate, direttamente o tramite fornitori IT, e ne rendiconta al PdC.
- **Funzione Acquisti e Legale**: inserisce i requisiti di sicurezza nei contratti, contribuisce con il PdC alla valutazione dei fornitori e alla predisposizione dell'elenco dei fornitori rilevanti.
- **Funzione Risorse Umane**: presidia le verifiche di affidabilità del personale, l'erogazione e la registrazione della formazione e l'applicazione delle misure disciplinari.
- **Funzione Privacy / DPO**: presidia la gestione delle violazioni di dati personali ai sensi degli artt. 33 e 34 del GDPR, in coordinamento con il processo di gestione degli incidenti.
- **Personale di M4**: rispetta le regole di sicurezza e segnala senza ritardo eventi, incidenti e debolezze osservate o sospettate.

7.4 Il Gestore del Servizio

ATM S.p.A. gestisce l'esercizio della Linea 4 e il relativo impianto tecnologico in forza del Contratto di gestione. Rispetto agli obblighi NIS2 di M4, ATM riveste tre qualità distinte:

- è il soggetto cui è affidata l'**attuazione operativa** delle misure di sicurezza sul dominio OT di linea;
- esercita, per delibera del CdA di M4, il ruolo di **Referente CSIRT** e dei relativi sostituti;
- è un **fornitore** di M4, di cui M4 tiene conto nella gestione del rischio della catena di approvvigionamento (cfr. §9.5).

ATM è a sua volta soggetto essenziale ai sensi del Decreto NIS2 e dispone di un proprio corpus di policy e procedure di sicurezza. Sul perimetro di M4 il Gestore deve:

- attuare i requisiti della presente Policy mediante processi documentati che si applicano esplicitamente al dominio OT di linea, rendendone disponibile la documentazione nel repository NIS2 di M4 (cfr. §8.3);
- sottoporre a M4 ogni modifica dell'infrastruttura, corredata di analisi del rischio, secondo quanto previsto dal Contratto di gestione;
- assicurare il monitoraggio 7x24 degli eventi di sicurezza del dominio OT di linea tramite un servizio SOC;
- gestire gli incidenti, informare tempestivamente il PdC ed effettuare le notifiche al CSIRT Italia per il tramite del Referente CSIRT;
- redigere e aggiornare il Risk Assessment del dominio OT di linea e le proposte di trattamento;
- rendicontare periodicamente a M4 secondo i flussi del §7.6;
- consentire le verifiche di M4, di soggetti da essa incaricati e dell'ACN, rendendo disponibili le evidenze;
- imporre ai propri subfornitori che operano sul perimetro di M4 requisiti almeno equivalenti.

L'individuazione delle strutture interne cui il Gestore affida le attività sul perimetro di M4 attiene all'organizzazione del Gestore e non è disciplinata dalla presente Policy. Il Gestore comunica al PdC i propri referenti per ciascuna area di attività e ne notifica tempestivamente le variazioni; M4 si relaziona con il Gestore esclusivamente in tale qualità, nei termini del Contratto di gestione.

7.5 Fornitori e manutentori

I fornitori e i manutentori che accedono ai sistemi di M4 o ne gestiscono componenti, sia per contratto diretto con M4 sia per il tramite del Gestore, devono:

- rispettare i requisiti di sicurezza previsti dal contratto e dal processo di sicurezza della catena di approvvigionamento;

- accedere ai sistemi solo con utenze nominative, autorizzate, protette da autenticazione forte e tracciate;
- segnalare senza ritardo, e comunque in tempi compatibili con il termine di preallarme di 24 ore, ogni incidente che interessi i sistemi di M4;
- consentire le verifiche di sicurezza previste dal contratto e vincolare a requisiti equivalenti gli eventuali subfornitori.

7.6 Coordinamento con il Gestore e flussi informativi

Il raccordo tra M4 e il Gestore si realizza attraverso un Tavolo di coordinamento cyber, convocato e presieduto dal PdC, cui partecipano la funzione tecnica responsabile del Contratto di gestione, la funzione IT di M4 e il Gestore del Servizio, con i referenti da esso designati, incluso il Referente CSIRT. Il Tavolo si riunisce almeno trimestralmente e, in via straordinaria, dopo ogni incidente significativo. Esamina lo stato delle misure e del piano di adeguamento, i rischi principali, gli incidenti, le vulnerabilità critiche, le eccezioni, le modifiche rilevanti e l'evoluzione normativa.

Flusso	Da	A	Tempistica
Segnalazione di incidente potenzialmente significativo	Gestore (SOC); funzione IT M4; fornitori	Referente CSIRT; PdC	Immediata non appena se ne viene a conoscenza, compatibile con il preallarme a 24 ore
Preallarme, notifica e relazione finale	Referente CSIRT	CSIRT Italia; copia al PdC	24 ore; 72 ore; un mese (art. 25)
Report di sicurezza del perimetro (indicatori, incidenti, vulnerabilità, eccezioni, stato delle misure)	Gestore; funzione IT M4	PdC	Semestrale
Risk Assessment e proposta di trattamento	Gestore; funzione IT M4	PdC, per l'approvazione del CdA	Annuale e a evento
Variazioni organizzative che incidono sui ruoli NIS2 o sui referenti del Gestore	M4; Gestore; Fornitori	PdC, per l'aggiornamento sul Portale NIS	In tempo utile per l'aggiornamento entro 14 giorni
Dati per gli adempimenti annuali ACN (registrazione, attività e servizi, fornitori rilevanti)	Funzioni M4; Gestore	PdC	Entro le finestre annuali ACN
Informativa sullo stato di attuazione	PdC	CdA	Almeno semestrale; tempestiva per incidenti significativi

Tabella 4 – Flussi informativi

7.7 Matrice RACI di macro-processo

La matrice sintetizza, a livello di macro-processo, l'attribuzione dei ruoli (R = Responsible, A = Accountable, C = Consulted, I = Informed). La documentazione dei processi declina la matrice a livello di singola attività e vi si raccorda; non può invertirne l'accountability.

Macro-processo	CdA	Rapp. Legale	PdC NIS2	Funzioni M4	Gestore del Servizio	Fornitori
Approvazione di Policy, piani ex art. 23 e Risk Assessment	A	C	R	C	–	–
Supervisione dell'attuazione e informativa agli organi	A	I	R	C	I	–
Governo del framework documentale e riesame annuale	I	I	A/R	C	C	–
Documentazione dei processi del dominio OT di linea	–	–	A	C	R	C
Relazioni con l'ACN e adempimenti sul Portale NIS	I	C	A/R	C	C	–
Valutazione e trattamento del rischio	I	–	A	R	R	C
Attuazione delle misure – dominio OT di linea (*)	I	–	A	C	R	R
Attuazione delle misure – dominio IT corporate	I	–	A	R	–	R
Monitoraggio e gestione degli incidenti – dominio OT (*)	I	–	A	I	R	C

Macro-processo	CdA	Rapp. Legale	PdC NIS2	Funzioni M4	Gestore del Servizio	Fornitori
Monitoraggio e gestione degli incidenti – dominio IT	I	–	A	R	–	R
Notifica degli incidenti significativi al CSIRT Italia (in caso di Servizio esternalizzato verso Gestore)	I	I	A	C	R	C
Sicurezza della catena di approvvigionamento	I	–	A	R	C	I
Formazione e consapevolezza	I	I	A	R	C	I
Verifiche, audit e piano di adeguamento	I	I	A	R	C	C

Tabella 5 – Matrice RACI di macro-processo

Nota. L'accountability (A) di ciascun macro-processo resta in capo a M4, coerentemente con la responsabilità degli organi di amministrazione ex art. 23 del Decreto NIS2. Il Gestore del Servizio e i fornitori operano in qualità di esecutori (R) o soggetti consultati (C), nei termini dei rispettivi contratti; il Gestore esercita inoltre il ruolo di Referente CSIRT affidatogli dal CdA. Nella colonna «Funzioni M4» il ruolo è esercitato dalla funzione competente per materia (cfr. §7.3).

(*) L'esecuzione da parte del Gestore delle attività di attuazione delle misure e di monitoraggio e gestione degli incidenti nel dominio OT di linea è subordinata alla preventiva approvazione delle varianti al Contratto di gestione e all'adeguamento del PEF.

8 - Sistema di gestione e architettura documentale

8.1 Il ciclo di gestione

M4 gestisce la sicurezza informatica secondo un ciclo Plan-Do-Check-Act, ricondotto agli obblighi del Decreto NIS2:

- **Plan** – valutazione del rischio, approvazione della Policy e dei piani da parte del CdA;
- **Do** – attuazione delle misure attraverso i processi indirizzati e il programma di adeguamento, strutturato in controlli, progettualità e macro-aree tematiche assegnate per ownership;
- **Check** – monitoraggio degli indicatori, verifiche e audit, riesame annuale della Policy (misura GV.PO-02);
- **Act** – piano di adeguamento (misura ID.IM-01), informativa agli organi e aggiornamento dei documenti.

L'approvazione della Policy e dei piani apre la fase di attuazione dei processi (ottobre 2026 – secondo trimestre 2027), cui segue il presidio continuo con mantenimento ed evoluzione (dal terzo trimestre 2027). Ogni processo va valutato e quantificato economicamente, per garantire risorse adeguate sia per la messa a regime sia per la manutenzione nel tempo, e le attività NIS2 affidate al Gestore vanno recepite nel Contratto di gestione.

8.2 Architettura documentale e repository NIS2

Livello	Contenuto	Approvazione	Predisposizione
1 – Indirizzo	Presente Policy, inclusa l'organizzazione per la sicurezza (cap. 7); atti di nomina dei ruoli NIS2	CdA	PdC
1 – Piani e rischio	Risk Assessment; piani ex art. 23: trattamento del rischio, gestione delle vulnerabilità, adeguamento, continuità operativa, ripristino in caso di disastro, gestione delle crisi, formazione, gestione degli incidenti	CdA	PdC con il supporto del Gestore per il dominio OT di linea; M4 per il dominio IT corporate
2 – Processi	Documentazione dei processi indirizzati (Allegato 1): procedure e istruzioni dei soggetti che li eseguono	PdC	PdC con il supporto del Gestore per il dominio OT di linea; M4 e fornitori IT per il dominio IT corporate
3 – Documenti operativi	Registri, inventari, elenchi, evidenze e documentazione tecnica	Owner di processo	Owner di processo

Tabella 6 – Architettura documentale

Tutta la documentazione dei livelli 1–3 è conservata nel **repository documentale NIS2 di M4**, che ne assicura la disponibilità per gli organi di amministrazione, gli organi di controllo e l'ACN. La presente Policy non elenca i singoli documenti: indirizza i processi, così che l'evoluzione della documentazione di attuazione non richieda

la revisione della Policy. Registri, inventari, elenchi e documentazione tecnico-operativa non richiedono l'approvazione del CdA, in coerenza con le indicazioni fornite dall'ACN.

8.3 Requisiti della documentazione dei processi

La documentazione di ciascun processo indirizzato, indipendentemente dal soggetto che la predispone, deve:

- dichiarare esplicitamente l'applicazione al perimetro di M4 e al dominio interessato;
- contenere una matrice RACI di attività raccordabile alla matrice del §7.7, senza inversioni di accountability, e indicare per ogni ruolo la struttura che esegue l'attività;
- essere redatta in forma prescrittiva, fissare parametri, soglie e frequenze verificabili e non inferiori a quelli della presente Policy;
- prevedere azioni di adeguamento (azione, owner, data obiettivo, stato, rischio residuo accettato nel frattempo), che alimentano il piano di adeguamento e il registro dei rischi;
- indicare le misure di base NIS2 pertinenti al processo;
- essere resa disponibile nel repository NIS2 di M4 e aggiornata a ogni variazione, con comunicazione al PdC.

9 - Ambiti di sicurezza: principi e processi indirizzati

Il presente capitolo disciplina i sedici ambiti previsti dalla misura GV.PO-01. Per ciascuno fissa l'obiettivo, i principi inderogabili e il processo cui è rinviato il dettaglio. L'Allegato 1 riepiloga la corrispondenza tra ambiti, misure di base, processi e soggetti esecutori per dominio.

9.1 Gestione del rischio

Misure di riferimento: GV.RM, GV.OC-04, ID.RA. **Obiettivo:** Identificare, valutare, trattare e monitorare i rischi per la sicurezza dei sistemi informativi e di rete di M4, incluse le dipendenze da fornitori e terze parti.

- la metodologia (scale, criteri di valutazione, soglie di accettazione) è unica per entrambi i domini ed è approvata dal CdA insieme al Risk Assessment;
- la valutazione comprende l'identificazione delle minacce e degli scenari di rischio ed è ripetuta almeno annualmente e in occasione di modifiche significative, incidenti significativi o nuove minacce;
- M4 mantiene un elenco aggiornato dei sistemi informativi e di rete rilevanti;
- il piano di trattamento indica per ogni rischio azione, owner, tempi e rischio residuo; l'accettazione del rischio residuo è formalizzata dal PdC entro le soglie approvate dal CdA e dal CdA oltre tali soglie.

Processo indirizzato: Processo di gestione del rischio cyber (valutazione e trattamento); piano di trattamento del rischio.

9.2 Ruoli e responsabilità

Misure di riferimento: GV.RR. **Obiettivo:** Assicurare che ruoli, responsabilità e poteri in materia di sicurezza informatica siano definiti, assegnati, conosciuti e dotati di risorse adeguate.

- ruoli e responsabilità sono definiti al cap. 7 e declinati nelle matrici RACI dei processi;
- le nomine dei ruoli NIS2 sono formalizzate e aggiornate sul Portale NIS entro 14 giorni da ogni variazione;
- le responsabilità affidate al Gestore e ai fornitori sono recepite nei rispettivi contratti.

Processo indirizzato: Modello organizzativo di cui al cap. 7; atti di nomina; Contratto di gestione.

9.3 Affidabilità delle risorse umane

Misure di riferimento: GV.RR-04. **Obiettivo:** Assicurare che il personale autorizzato ad accedere ai sistemi rilevanti, e in particolare gli amministratori di sistema, sia valutato per esperienza, capacità e affidabilità.

- le verifiche di affidabilità sono svolte prima dell'assegnazione del ruolo e ripetute periodicamente, nel rispetto della normativa applicabile;
- l'ingresso, il cambio di mansione e l'uscita del personale attivano l'assegnazione, la modifica e la revoca degli accessi;
- requisiti equivalenti sono imposti per contratto al personale del Gestore e dei fornitori che opera sul perimetro di M4.

Processo indirizzato: Processo di sicurezza delle risorse umane e degli amministratori di sistema.

9.4 Conformità e audit di sicurezza

Misure di riferimento: GV.OV, GV.PO-02, ID.IM-01. **Obiettivo:** Verificare nel continuo l'adeguatezza e l'effettiva applicazione delle misure e pianificarne l'adeguamento.

- M4 adotta un programma annuale di verifiche che copre entrambi i domini, il Gestore e i fornitori rilevanti;
- la Policy e la documentazione dei processi sono riesaminate almeno annualmente, anche per verificarne la conformità normativa;
- il piano di adeguamento raccoglie le azioni che derivano da Risk Assessment, verifiche, incidenti e azioni di adeguamento dei processi, ed è oggetto di informativa agli organi.

Processo indirizzato: Processo di verifica, audit e riesame della conformità; piano di adeguamento.

9.5 Sicurezza della catena di approvvigionamento

Misure di riferimento: GV.SC. **Obiettivo:** Gestire i rischi derivanti da fornitori e terze parti, incluso il Gestore del Servizio.

- M4 mantiene l'inventario dei fornitori e l'elenco dei fornitori rilevanti comunicato annualmente all'ACN;
- i fornitori sono valutati prima del contratto e periodicamente, in proporzione alla criticità della fornitura;
- i contratti includono requisiti di sicurezza, obblighi di notifica degli incidenti, diritto di verifica, regole sulla subfornitura e obblighi alla cessazione del rapporto, e definiscono ruoli e responsabilità del personale del fornitore;
- il Contratto di gestione è adeguato per recepire gli obblighi NIS2 affidati al Gestore.

Processo indirizzato: Processo di sicurezza della catena di approvvigionamento.

9.6 Gestione degli asset

Misure di riferimento: ID.AM. **Obiettivo:** Conoscere e governare gli asset hardware, software, i servizi e i flussi di dati del perimetro.

- M4 dispone di inventari completi e aggiornati di hardware, software, servizi e flussi di dati per entrambi i domini, con un owner per ciascun asset;
- per il dominio OT di linea l'inventario è mantenuto dal Gestore ed è reso disponibile a M4, titolare degli asset;
- gli asset sono classificati per criticità e gestiti lungo tutto il ciclo di vita, fino alla dismissione sicura.

Processo indirizzato: Processo di gestione degli asset.

9.7 Gestione delle vulnerabilità

Misure di riferimento: ID.RA-01, ID.RA-08, PR.PS-02. **Obiettivo:** Individuare, valutare e trattare le vulnerabilità in tempi commisurati al rischio.

- le vulnerabilità sono individuate con continuità, con tecniche compatibili con i sistemi OT, e alimentate dalle fonti informative dei produttori e del CSIRT Italia;
- la priorità di trattamento dipende dalla criticità della vulnerabilità e dell'asset; i tempi massimi di rimedio sono fissati per classe di criticità;
- gli aggiornamenti sui sistemi OT sono verificati prima dell'installazione; l'impossibilità tecnica di applicarli è gestita come eccezione con misure compensative;
- M4 dispone di un canale per ricevere segnalazioni di vulnerabilità da terzi.

Processo indirizzato: Processo di gestione delle vulnerabilità e degli aggiornamenti; piano di gestione delle vulnerabilità.

9.8 Continuità operativa, ripristino in caso di disastro e gestione delle crisi

Misure di riferimento: ID.IM-04, PR.DS-11, RC. **Obiettivo:** Assicurare la continuità dei servizi e il ripristino dei sistemi in caso di incidente, disastro o crisi.

- i piani di continuità operativa, di ripristino in caso di disastro e di gestione delle crisi sono approvati dal CdA e coordinati con i piani di esercizio del Gestore e con gli obblighi CER;
- per i sistemi rilevanti sono definiti tempi e punti di ripristino (RTO/RPO) coerenti con l'analisi di impatto;
- i dati e le configurazioni sono salvati con copie protette e isolate, e il ripristino è provato periodicamente;
- i piani sono esercitati almeno annualmente e aggiornati sulla base degli esiti.

Processo indirizzato: Processi di continuità operativa, ripristino in caso di disastro, gestione delle crisi e backup & restore; piani di continuità operativa, di ripristino in caso di disastro e di gestione delle crisi.

9.9 Identità digitali e controllo degli accessi

Misure di riferimento: PR.AA. **Obiettivo:** Garantire che solo utenti, processi e dispositivi autorizzati accedano ai sistemi, con i privilegi strettamente necessari.

- le utenze sono nominative e univoche; l'accesso è concesso secondo i principi del need-to-know e del privilegio minimo, su profili basati sui ruoli;
- l'autenticazione a più fattori è obbligatoria per gli accessi remoti e per gli accessi con privilegi amministrativi, inclusi quelli dei fornitori verso gli impianti;
- gli accessi dei fornitori al dominio OT di linea avvengono solo attraverso punti di accesso controllati e tracciati;
- le utenze locali degli impianti sono censite; le credenziali di default sono modificate e le utenze condivise sono ammesse solo come eccezione registrata;
- le abilitazioni sono riesaminate periodicamente e revocate tempestivamente quando non più necessarie.

Processo indirizzato: Processo di gestione delle autenticazioni, delle identità e degli accessi digitali.

9.10 Sicurezza fisica

Misure di riferimento: PR.AA-06. **Obiettivo:** Proteggere dall'accesso fisico non autorizzato i locali e gli apparati che ospitano i sistemi informativi e di rete.

- i locali tecnici, le sale apparati, il posto centrale di controllo e gli armadi di stazione sono ad accesso controllato e registrato;
- gli accessi fisici di fornitori e manutentori sono autorizzati, accompagnati ove necessario e tracciati;
- le misure sono coordinate con la sicurezza fisica della linea e con gli obblighi CER.

Processo indirizzato: Processo di sicurezza fisica dei locali e degli apparati.

9.11 Formazione e consapevolezza

Misure di riferimento: PR.AT. **Obiettivo:** Assicurare che organi di amministrazione, personale e ruoli specializzati abbiano competenze adeguate in materia di sicurezza informatica.

- il piano di formazione copre gli organi di amministrazione, tutto il personale di M4 e, con percorsi dedicati, i ruoli specializzati;
- la partecipazione è registrata e i contenuti sono aggiornati almeno annualmente;
- requisiti formativi equivalenti sono imposti per contratto al personale del Gestore e dei fornitori che opera sul perimetro.

Processo indirizzato: Processo di formazione e consapevolezza; piano di formazione.

9.12 Sicurezza dei dati

Misure di riferimento: PR.DS. **Obiettivo:** Proteggere riservatezza, integrità e disponibilità dei dati a riposo, in transito e in uso.

- le informazioni sono classificate e protette in funzione della classificazione;
- i dati sono cifrati in transito su reti esterne e negli accessi remoti e, per le informazioni critiche, a riposo, con una gestione sicura delle chiavi;
- i supporti e i dispositivi dismessi o riutilizzati sono sottoposti a cancellazione sicura;
- i trattamenti di dati personali rispettano il GDPR, con il coinvolgimento del DPO.

Processo indirizzato: Processo di sicurezza dei dati e di gestione della crittografia.

9.13 Sviluppo, configurazione, manutenzione e dismissione dei sistemi

Misure di riferimento: PR.PS. **Obiettivo:** Garantire che la sicurezza sia integrata in tutto il ciclo di vita dei sistemi, dalla progettazione alla dismissione.

- i requisiti di sicurezza sono definiti in fase di progettazione e di acquisto (security by design);
- per ciascuna classe di asset esiste una configurazione di sicurezza di riferimento documentata, la cui applicazione è verificata con frequenza definita;
- le modifiche sono autorizzate, provate e tracciate; nel dominio OT di linea sono sottoposte all'autorizzazione di M4, con analisi del rischio predisposta dal Gestore e, in presenza di impatti sulla sicurezza, valutazione del PdC;
- sono installati solo software autorizzati e i sistemi generano i log necessari al monitoraggio.

Processo indirizzato: Processi di hardening, di sviluppo sicuro del software e di gestione delle modifiche.

9.14 Protezione delle reti e delle comunicazioni

Misure di riferimento: PR.IR, PR.DS-02. **Obiettivo:** Proteggere reti e comunicazioni da accessi e flussi non autorizzati e assicurarne la resilienza.

- il dominio OT di linea è separato dalle reti esterne e dal dominio IT ed è segmentato in zone e condotti secondo IEC 62443;
- i flussi sono limitati allo stretto necessario; i firewall a presidio del dominio OT sono gestiti in via unitaria;
- ogni interconnessione con reti esterne è autorizzata da M4;
- le componenti critiche di rete sono ridondate in coerenza con i requisiti di disponibilità dell'esercizio.

Processo indirizzato: Processo di sicurezza delle reti.

9.15 Monitoraggio degli eventi di sicurezza

Misure di riferimento: DE.CM, DE.AE. **Obiettivo:** Rilevare tempestivamente eventi anomali e potenziali incidenti.

- gli eventi di sicurezza dei sistemi rilevanti di entrambi i domini sono raccolti in modo centralizzato, conservati per un periodo adeguato e protetti da alterazione;
- gli eventi rilevati sono analizzati e, se del caso, gestiti come incidenti.

Processo indirizzato: Processo di monitoraggio e tracciamento degli eventi di sicurezza.

9.16 Risposta agli incidenti e ripristino

Misure di riferimento: RS, RC. **Obiettivo:** Gestire gli incidenti in modo da contenerne gli effetti, ripristinare i servizi e adempiere agli obblighi di notifica.

- il processo di gestione degli incidenti è unico per entrambi i domini, con classificazione di severità e qualificazione di significatività secondo le Determinazioni ACN;
- gli incidenti significativi sono notificati al CSIRT Italia dal Referente CSIRT: preallarme entro 24 ore, notifica entro 72 ore, relazione finale entro un mese;
- le violazioni di dati personali sono gestite in coordinamento con il DPO ai sensi degli artt. 33 e 34 del GDPR;
- ogni incidente significativo è oggetto di informativa tempestiva al CdA e di analisi delle cause, i cui esiti alimentano il piano di adeguamento.

Processo indirizzato: Processo di gestione e notifica degli incidenti; piano per la gestione degli incidenti.

10 - Informativa agli organi di amministrazione

Il PdC predispone per il CdA un'informativa almeno semestrale sullo stato della sicurezza informatica di M4, che comprende:

- lo stato di attuazione delle misure e del piano di adeguamento;
- i rischi principali e il rischio residuo accettato;
- gli incidenti occorsi, con evidenza di quelli notificati al CSIRT Italia;
- gli esiti delle verifiche e degli audit;
- le eccezioni in essere;
- lo stato della formazione, inclusa quella degli organi di amministrazione;
- l'evoluzione del quadro normativo e delle Determinazioni ACN;
- i fabbisogni di risorse e gli adeguamenti necessari del Contratto di gestione.

Gli incidenti significativi sono oggetto di informativa tempestiva, indipendentemente dalla cadenza periodica.

11 - Eccezioni e violazioni

11.1 Gestione delle eccezioni

Quando un requisito della presente Policy o della documentazione di un processo non può essere applicato per ragioni tecniche, operative o contrattuali, la deroga deve essere:

- motivata e accompagnata da una valutazione del rischio;
- corredata di misure compensative;
- approvata dal PdC; per il dominio OT di linea, su istruttoria del Gestore del Servizio;
- limitata nel tempo, con durata non superiore a dodici mesi, rinnovabile solo previo riesame;
- registrata nel registro delle eccezioni e riportata nell'informativa al CdA.

Le eccezioni che comportano un rischio residuo superiore alle soglie approvate dal CdA richiedono l'accettazione del CdA.

11.2 Violazioni

Il mancato rispetto della presente Policy da parte del personale di M4 può comportare l'applicazione di provvedimenti disciplinari, secondo la normativa e i contratti collettivi applicabili.

12 - Aggiornamento e gestione della documentazione

12.1 Aggiornamento

La presente Policy è riesaminata dal PdC almeno annualmente (misura GV.PO-02) e, in ogni caso, in occasione di:

- variazioni del quadro normativo o delle Determinazioni ACN;
- variazioni organizzative di M4 o del Gestore che incidano sui ruoli;
- modifiche del Contratto di gestione;
- incidenti significativi o esiti di verifiche che evidenzino carenze del modello.

Le modifiche sostanziali sono approvate dal CdA. L'aggiornamento degli allegati conseguente a variazioni delle Determinazioni ACN o dei processi indirizzati è curato dal PdC e portato a conoscenza del CdA nella prima informativa utile.

12.2 Gestione della documentazione

La presente Policy e i documenti che ne discendono sono conservati, con gestione delle versioni, nel repository documentale NIS2 di M4 e sono resi disponibili ai destinatari per quanto di rispettiva competenza. Le evidenze di attuazione sono conservate dagli owner di processo e rese disponibili a M4, agli organi di controllo e all'ACN.

13 - Allegati

13.1 Allegato 1 – Mappa degli ambiti e dei processi indirizzati

N.	Ambito (GV.PO-01)	Misure di riferimento	Processo indirizzato	Esecuzione – dominio OT di linea	Esecuzione – dominio IT corporate
1	Gestione del rischio	GV.RM, GV.OC-04, ID.RA	Processo di gestione del rischio cyber (valutazione e trattamento); piano di trattamento del rischio.	Gestore	M4
2	Ruoli e responsabilità	GV.RR	Modello organizzativo di cui al cap. 7; atti di nomina; Contratto di gestione.	M4	M4

N.	Ambito (GV.PO-01)	Misure di riferimento	Processo indirizzato	Esecuzione – dominio OT di linea	Esecuzione – dominio IT corporate
3	Affidabilità delle risorse umane	GV.RR-04	Processo di sicurezza delle risorse umane e degli amministratori di sistema.	Gestore, per il proprio personale	M4 e fornitori IT
4	Conformità e audit di sicurezza	GV.OV, GV.PO-02, ID.IM-01	Processo di verifica, audit e riesame della conformità; piano di adeguamento.	M4, con il contributo del Gestore	M4
5	Sicurezza della catena di approvvigionamento	GV.SC	Processo di sicurezza della catena di approvvigionamento.	M4; Gestore per i propri subfornitori	M4
6	Gestione degli asset	ID.AM	Processo di gestione degli asset.	Gestore per gli asset dati in gestione e secondo quanto previsto nel Contratto di gestione	M4 e fornitori IT
7	Gestione delle vulnerabilità	ID.RA-01, ID.RA-08, PR.PS-02	Processo di gestione delle vulnerabilità e degli aggiornamenti; piano di gestione delle vulnerabilità.	Gestore secondo quanto previsto nel Contratto di gestione	M4 e fornitori IT
8	Continuità operativa, ripristino in caso di disastro e gestione delle crisi	ID.IM-04, PR.DS-11, RC	Processi di continuità operativa, ripristino in caso di disastro, gestione delle crisi e backup & restore; piani di continuità operativa, di ripristino in caso di disastro e di gestione delle crisi.	Gestore secondo quanto previsto nel Contratto di gestione	M4 e fornitori IT
9	Identità digitali e controllo degli accessi	PR.AA	Processo di gestione delle autenticazioni, delle identità e degli accessi digitali.	Gestore secondo quanto previsto nel Contratto di gestione	M4 e fornitori IT
10	Sicurezza fisica	PR.AA-06	Processo di sicurezza fisica dei locali e degli apparati.	Gestore secondo quanto previsto nel Contratto di gestione	M4
11	Formazione e consapevolezza	PR.AT	Processo di formazione e consapevolezza; piano di formazione.	Gestore, per il proprio personale e secondo quanto previsto nel Contratto di gestione	M4, per il personale e gli organi di M4
12	Sicurezza dei dati	PR.DS	Processo di sicurezza dei dati e di gestione della crittografia.	Gestore secondo quanto previsto nel Contratto di gestione	M4 e fornitori IT
13	Sviluppo, configurazione, manutenzione e dismissione dei sistemi	PR.PS	Processi di hardening, di sviluppo sicuro del software e di gestione delle modifiche.	Gestore secondo quanto previsto nel Contratto di gestione; autorizzazione delle modifiche da parte di M4	M4 e fornitori IT
14	Protezione delle reti e delle comunicazioni	PR.IR, PR.DS-02	Processo di sicurezza delle reti.	Gestore secondo quanto previsto nel Contratto di gestione	M4 e fornitori IT
15	Monitoraggio degli eventi di sicurezza	DE.CM, DE.AE	Processo di monitoraggio e tracciamento degli eventi di sicurezza.	Gestore secondo quanto previsto nel Contratto di gestione	M4 e fornitori IT/OT
16	Risposta agli incidenti e ripristino	RS, RC	Processo di gestione e notifica degli incidenti; piano per la gestione degli incidenti.	Gestore secondo quanto previsto nel Contratto di gestione; notifica tramite Referente CSIRT secondo quanto previsto dal Contratto CSIRT	M4 e fornitori IT/OT; notifica tramite Referente CSIRT

Tabella 7 – Ambiti, misure, processi indirizzati ed esecuzione per dominio

La documentazione di attuazione di ciascun processo è conservata nel repository documentale NIS2 di M4. La responsabilità del processo resta in capo a M4 secondo la matrice del §7.7.

13.2 Allegato 2 – Compliance NIS2

Il presente Allegato costituisce parte integrante della Policy e raccoglie i riferimenti normativi NIS2 e le misure di sicurezza di base ACN indirizzate dalla Policy. È aggiornato in funzione dell'evoluzione delle Determinazioni ACN, ferme restando le parti della Policy che disciplinano organizzazione e responsabilità.

Quadro normativo di riferimento

- Direttiva (UE) 2022/2555 (c.d. Direttiva NIS2);
- D.Lgs. 4 settembre 2024, n. 138 – recepimento della Direttiva NIS2, artt. 7, 23, 24, 25 e 30.

Determinazioni ACN di riferimento (fonte: acn.gov.it/portale/nis/la-normativa)

- n. 164179 del 14/04/2025 – misure di sicurezza e incidenti significativi di base;
- n. 379907 del 19/12/2025 – misure di sicurezza e tassonomia degli incidenti;
- n. 379887 del 19/12/2025 – piattaforma digitale (sostituisce la n. 333017 del 22/09/2025);

- n. 127434 e n. 127437 del 13/04/2026 – scadenze per i soggetti 2026 e fornitori rilevanti;
- n. 155238/2026 – elencazione e categorizzazione delle attività e dei servizi.

Misure di base indirizzate direttamente dalla Policy

Misura	Contenuto	Presidio nella Policy
GV.OC-04	Elenco aggiornato dei sistemi informativi e di rete rilevanti	§3.2; §9.1
GV.RM	Strategia e piano di gestione dei rischi per la sicurezza informatica	§9.1; §8.2
GV.RR-02	Organizzazione della sicurezza informatica, ruoli, responsabilità e punto di contatto	Cap. 7
GV.RR-04	Affidabilità del personale autorizzato, inclusi gli amministratori di sistema	§9.3
GV.PO-01	Politiche di sicurezza informatica sugli ambiti previsti	Cap. 9; Allegato 1
GV.PO-02	Riesame annuale delle politiche	§12.1
GV.OV	Supervisione degli organi sulla strategia di sicurezza informatica	Cap. 10
GV.SC	Gestione del rischio della catena di approvvigionamento	§7.4; §7.5; §9.5
ID.IM-01	Piano di adeguamento e informativa agli organi di amministrazione	§8.1; §9.4; cap. 10
PR.AT-01	Piano di formazione, esteso agli organi di amministrazione	§7.2; §9.11

Tabella 8 – Misure di base indirizzate direttamente dalla Policy

Le misure di base pertinenti ai singoli ambiti sono indicate nella documentazione di ciascun processo indirizzato.