Codice A1500B
D.D. 30 ottobre 2026, n. 527
D.Lgs. 4 settembre 2024 n. 138. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica. Approvazione dell'impianto documentale NIS da parte degli organi di amministrazione e direttivi di cui all'articolo 23, comma 1, lett. a) del Decreto NIS

ATTO DD 527/A1500B/2026 DEL 30/10/2026

DETERMINAZIONE DIRIGENZIALE
A1500B - ISTRUZIONE E DIRITTO ALLO STUDIO UNIVERSITARIO, FORMAZIONE E LAVORO

OGGETTO: D.Lgs. 4 settembre 2024 n. 138. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica. Approvazione dell'impianto documentale NIS da parte degli organi di amministrazione e direttivi di cui all'articolo 23, comma 1, lett. a) del Decreto NIS

Premesso che:

- La Direttiva (UE) 2022/2555 (NIS 2) del Parlamento Europeo e del Consiglio, stabilisce misure volte a garantire un livello comune elevato di cybersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno, definendo una serie di obblighi e misure da adottare da parte degli Stati membri;

- il D.Lgs. 4 settembre 2024 n. 138, , anche definito "Decreto NIS", recepisce la direttiva (UE) 2022/2555 (NIS 2), e dispone all'art 3, comma 6 che "Il presente decreto si applica, altresì, anche indipendentemente dalle loro dimensioni, alle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III";

- il sopra richiamato "Decreto NIS" dispone all'art. 6, comma 3 che "sono considerati soggetti importanti i soggetti di cui all'articolo 3 che non sono considerati essenziali ai sensi dei commi 1 e 2 del presente articolo";

- il D.Lgs. 4 settembre 2024 n. 138, all'art 23 espressamente sancisce che gli organi di amministrazione e gli organi direttivi dei soggetti importanti "approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24";

- il "Decreto NIS" prevede altresì all'art 24 che i soggetti importanti "adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri

servizi";

- il D.Lgs. 4 settembre 2024 n. 138, all'art 38, comma 6, in caso di violazione delle disposizioni in esso contenute, stabilisce l'applicazione delle sanzioni amministrative nei confronti delle persone fisiche "ivi inclusi agli organi di amministrazione e gli organi direttivi di cui all'articolo 23 dei soggetti essenziali e dei soggetti importanti, nonché di quelle che svolgono funzioni dirigenziali a livello di amministratore delegato o rappresentante legale di un soggetto essenziale o importante" .

Premesso inoltre che:

- ai sensi dell'articolo 7, comma 1, lettera c), del "decreto NIS" il Presidente della Regione Piemonte ha delegato in data 19 febbraio 2025, tramite atto di delega resa in forma di dichiarazione sostitutiva di Atto di Notorietà, ex articolo 47 del D.P.R. n. 445/2000, quale "Punto di contatto" il Responsabile del Settore "Sistema informativo regionale" di Regione Piemonte, nominato con DGR 3-474 del 03 dicembre 2024 "Referente per la Cybersicurezza", in ottemperanza all'articolo 8 della legge n. 90/2024.

- la D.G.R.- n. 15-1430 del 28 luglio 2025 "Decreto legislativo n. 138/2024. Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale n. 136430 del 12 aprile 2025, di riconoscimento della Regione Piemonte quale entità critica per la cybersicurezza nazionale. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica" ha individuato i soggetti da indicare nella sezione del Portale NIS appositamente dedicata all'elencazione degli organi amministrativi e direttivi dell'Ente, come previsto dall'articolo 23 comma 1, lettera c), del medesimo del "decreto NIS";

- la D.G.R. sopra richiamata ha disposto di rinviare a successivi provvedimenti le valutazioni di impatto dei necessari interventi in materia.

Considerato che:

- le disposizioni di cui al D.Lgs. 4 settembre 2024 n. 138 si applicano anche a Regione Piemonte in virtù del disposto dell'art. 3 comma 6 e dell'allegato III del decreto legislativo stesso;

- Regione Piemonte è considerato "soggetto importante" ai fini dell'applicazione della normativa di riferimento per le ragioni di cui in premessa;

- nel mese di ottobre 2026 è fissato il termine ultimo per l'attuazione delle misure di sicurezza di base, in conformità al periodo di 18 mesi decorrente dalla data della comunicazione via PEC di inserimento nell'elenco dei soggetti NIS;

- l'obbligo di approvazione dell'impianto documentale, coerente con le FAQ ACN ODA.10 e le linee guida NIS sulle specifiche di base non è delegabile, in quanto la normativa vigente e le indicazione ACN presenti nelle FAQ ODA.8 attribuiscono esclusivamente agli organi di amministrazione e direttivi la responsabilità collegiale di approvare tali atti. Tale obbligo, infatti, rimane in capo agli organi suddetti e non può essere trasferito né a singoli membri, né ad altri organi o funzioni del soggetto NIS, indipendentemente dal modello di governance adottato dall'Ente;

Considerato inoltre che

- Per adempiere a tali obblighi, il Referente per la Cybersicurezza ha predisposto, grazie alla collaborazione del Gruppo di lavoro interdirezionale “Attuazione della normativa in materia di Cybersicurezza”, istituito con Determinazione Dirigenziale n. 11/A1000A/2025 del 22/01/2025, un impianto documentale organico, conforme ai requisiti delle misure di sicurezza, che ne richiede l’approvazione e comprende i seguenti elementi:

- Organizzazione per la sicurezza informatica
- Politiche di sicurezza informatica
- Valutazione del rischio relativo alla sicurezza dei sistemi informativi e di rete
- Piano di trattamento del rischio
- Piano di gestione delle vulnerabilità
- Piano di adeguamento
- Piano di continuità operativa
- Piano di ripristino in caso di disastro
- Piano di gestione delle crisi
- Piano di formazione
- Piano per la gestione degli incidenti di sicurezza informatica

Gli organi amministrativi di vertice, come individuati dal decreto legislativo 138/2024, hanno:

- già provveduto ad approvare il **Piano per la gestione degli incidenti di sicurezza informatica**, attraverso validazione da parte del Comitato di Coordinamento dei Direttori in data 16 dicembre 2025 e successiva approvazione mediante Determinazione Dirigenziale da parte di ciascun Direttore regionale;
- condiviso, esaminato e validato i restanti documenti dell’**impianto documentale NIS** nella seduta del Comitato di Coordinamento dei Direttori tenutasi il 6 ottobre 2026, stabilendo di procedere alla loro adozione e approvazione con successivo specifico atto.

Ritenuto opportuno, per quanto sopra esposto:

- approvare per la Direzione Istruzione e Diritto allo Studio universitario, Formazione e Lavoro l’impianto documentale sopra elencato condiviso in sede di Comitato di Coordinamento Direttori e contenente le funzioni di gestione, indirizzo e pianificazione strategica che riflettono e declinano i requisiti delle misure di sicurezza di cui agli obblighi riferiti ai “soggetti importanti” come Regione Piemonte.

- dare effettiva attuazione ai documenti, mantenendo un costante rapporto con il Referente per la Cybersicurezza e le strutture organizzative dell’Ente competenti per materia.

Attestato che, in esito all’istruttoria sopra richiamata, il presente provvedimento non comporta effetti contabili diretti né effetti prospettici sulla gestione finanziaria, economica e patrimoniale della Regione Piemonte.

Tutto ciò premesso e considerato

IL DIRETTORE

Richiamati i seguenti riferimenti normativi:

- il decreto legislativo n. 82/2005 "Codice dell'Amministrazione Digitale";

- il decreto legislativo n. 196/2003 "Codice in materia di protezione dei dati personali";
- la legge n. 190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";
- la L. 2 luglio 2024 n. 90 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici";
- la deliberazione della Giunta regionale n. 3-2182/2026/XII del 30/01/2026: Approvazione del Piano integrato di attività e organizzazione (PIAO) della Giunta regionale del Piemonte per gli anni 2026-2028, ai sensi del Decreto Legge n. 80 del 9 giugno 2021, convertito in Legge n. 113 del 6 agosto 2021.;
- il regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR);
- il D.Lgs. 4 settembre 2024 n. 138 "Decreto Legislativo e regolamenti associati per l'adozione della Diretiva NIS2";
- la D.G.R.- n. 15-1430 del 28 luglio 2025 "Decreto legislativo n. 138/2024. Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale n. 136430 del 12 aprile 2025, di riconoscimento della Regione Piemonte quale entità critica per la cybersicurezza nazionale. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica";
- la D.D. 22 gennaio 2025, n. 11 "Istituzione del Gruppo di lavoro interdirezionale "Attuazione della normativa in materia di Cybersicurezza"';

determina

per le motivazioni in premessa che integralmente e sostanzialmente si richiamano:

- di prendere atto del verbale del Comitato di Coordinamento Direttori del 06/10/2026 con il quale sono stati condivisi, esaminati e validati i documenti che verranno approvati dagli organi di amministrazione e direttivi di cui all’articolo 23, comma 1, lett. a) del decreto NIS;

- di approvare e adottare per la Direzione Istruzione e Diritto allo Studio universitario, Formazione e Lavoro come convenuto, i seguenti documenti:

  - Organizzazione per la sicurezza informatica
  - Politiche di sicurezza informatica
  - Valutazione del rischio relativo alla sicurezza dei sistemi informativi e di rete
  - Piano di trattamento del rischio
  - Piano di gestione delle vulnerabilità
  - Piano di adeguamento
  - Piano di continuità operativa
  - Piano di ripristino in caso di disastro
  - Piano di gestione delle crisi
  - Piano di formazione

, di cui all’Allegato 1, parte integrante e sostanziale della presente provvedimento per quanto di competenza;

La presente determinazione non è soggetta alla pubblicazione ai sensi del Decreto Legislativo

33/2013, in materia di trasparenza nella pubblica amministrazione.

La presente determinazione sarà pubblicata sul Bollettino ufficiale della Regione Piemonte ai sensi dell'articolo 61 dello Statuto e dell' art. 5 della legge regionale 12 ottobre 2010, n. 22.

IL DIRETTORE (A1500B - ISTRUZIONE E DIRITTO ALLO STUDIO UNIVERSITARIO, FORMAZIONE E LAVORO)
Firmato digitalmente da Giovanni Bocchieri

Si dichiara che sono parte integrante del presente provvedimento gli allegati riportati a seguire [1], archiviati come file separati dal testo del provvedimento sopra riportato:

1. REGP_PIA01_Piano_Gestione_IncidentiSicurezza-IT_v02feb.pdf
2. REGP_PIA02_Piano_di_gestione_delle_vulnerabilità_v01.pdf
3. REGP_PIA03_Valutazione_Rischio_Cyber_v01.pdf
4. REGP_PIA04_Piano_Trattamento_Rischi_v01.pdf
5. REGP_PIA05_Piano_Adeguamento_NIS2_v01.pdf
6. REGP_PIA06_Piano_di_formazione_Sicurezza_Infomatica_v02.pdf
7. REGP_PIA07_Piano_Continuita_Operativa_v06.pdf
8. REGP_PIA08_Piano_di_Ripristino_in_caso_di_disastro_v5.pdf
9. REGP_PIA09_Piano_di_Gestione_delle_Crisi_v05.pdf
10. REGP_POL01_Organizzazione_per_la_sicurezza_informatica_v01.pdf
11. REGP_POL02_Politiche_Sicurezza_Informatica_v01.pdf

Allegato

1 L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento

VERIFICHE ED APPROVAZIONI

VER.	REDAZIONE		CONTROLLO ED APPROVAZIONE		AUTORIZZAZIONE ALL'EMISSIONE	
	NOME	DATA	NOME	DATA	NOME	DATA
V01			Coordinamento Direttori	16/12/2025	Giunta Regionale	

STATO DELLE VARIAZIONI

VER.	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
V01	Tutto il documento	Versione iniziale del documento

INDICE

SCOPO DEL DOCUMENTO....3

CAMPO DI APPLICAZIONE....3

GLOSSARIO E RIFERIMENTI INTERNI....4

1.1 GLOSSARIO DEI TERMINI....4
1.1 GLOSSARIO DEI TERMINI....4

RIFERIMENTI TECNICI E ORGANIZZATIVI....5

1.2 RIFERIMENTI INTERNI....5
1.2 RIFERIMENTI INTERNI....5

PRINCIPI DI GESTIONE E POLITICHE....6

RUOLI E RESPONSABILITÀ....7

GESTIONE, COMUNICAZIONE E NOTIFICA DEGLI INCIDENTI....8

1.3 PROCESSO DI GESTIONE DEGLI INCIDENTI DI SICUREZZA....8
1.3 PROCESSO DI GESTIONE DEGLI INCIDENTI DI SICUREZZA....8
1.4 FUNZIONI DA CUI PUÒ PERVENIRE LA SEGNALAZIONE DI UN INCIDENTE....9
1.4 FUNZIONI DA CUI PUÒ PERVENIRE LA SEGNALAZIONE DI UN INCIDENTE....9
1.4.1 Rilevazione e Segnalazione....9
1.4.1 Rilevazione e Segnalazione....9
1.4.2 Classificazione e Analisi....9
1.4.2 Classificazione e Analisi....9
1.4.3 Contenimento e Mitigazione....10
1.4.3 Contenimento e Mitigazione....10
1.4.4 Comunicazione e Notifica....10
1.4.4 Comunicazione e Notifica....10
1.4.5 Risoluzione, Ripristino e Chiusura....10
1.4.5 Risoluzione, Ripristino e Chiusura....10
1.4.6 Reporting e Miglioramento Continuo....10
1.4.6 Reporting e Miglioramento Continuo....10
1.4.7 Matrice RACI – Ruoli e Responsabilità....11
1.4.7 Matrice RACI – Ruoli e Responsabilità....11

1.5 INCIDENTI SIGNIFICATIVI PER CUI È RICHIESTA LA NOTIFICA....12
1.5 INCIDENTI SIGNIFICATIVI PER CUI È RICHIESTA LA NOTIFICA....12
1.6 NOTIFICA VERSO AUTORITÀ E ORGANISMI NAZIONALI....12
1.6 NOTIFICA VERSO AUTORITÀ E ORGANISMI NAZIONALI....12
1.7 COMUNICAZIONE VERSO STRUTTURE INTERNE INTERESSATE, ARTICOLAZIONI COMPETENTI, ENTI FRUITORI E ISTITUZIONI....13
1.7 COMUNICAZIONE VERSO STRUTTURE INTERNE INTERESSATE, ARTICOLAZIONI COMPETENTI, ENTI FRUITORI E ISTITUZIONI....13
1.7.1 Comunicazione interna....14
1.7.1 Comunicazione interna....14
1.7.2 Comunicazione pubblica e relazioni esterne....14
1.7.2 Comunicazione pubblica e relazioni esterne....14
1.8 TRACCIABILITÀ E RISERVATEZZA....15
1.8 TRACCIABILITÀ E RISERVATEZZA....15
REPORTING E RIESAME....15
1.9 REPORTING PERIODICO AL COORDINAMENTO DIRETTORI....15
1.9 REPORTING PERIODICO AL COORDINAMENTO DIRETTORI....15
MIGLIORAMENTO CONTINUO....16
1.10 DIFFUSIONE E CONSAPEVOLEZZA....16
1.10 DIFFUSIONE E CONSAPEVOLEZZA....16

SCOPO DEL DOCUMENTO

La direttiva (UE) 2022/2555 (Direttiva NIS 2), volta a stabilire misure per un livello comune elevato di cibersicurezza nell'Unione, e il relativo decreto di attuazione (D.Lgs 4 settembre 2024, n. 138), si rivolgono essenzialmente a due categorie di soggetti, i Soggetti Importanti e i Soggetti Essenziali. A tali soggetti la direttiva impone specifici oneri:

- adozione di misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi;
- obbligo di notifica, senza ingiustificato ritardo, al CSIRT Italia di ogni incidente che abbia un impatto significativo sulla fornitura dei loro servizi.

Il presente *Piano di Gestione degli Incidenti di Sicurezza IT* definisce i principi, le responsabilità e il modello di governance adottato dalla **Regione Piemonte** per assicurare una gestione efficace, coordinata e conforme alla normativa vigente degli incidenti di sicurezza informatica.
L'obiettivo è garantire:

- la **protezione della continuità operativa** dei servizi digitali erogati;
- la **tutela della riservatezza, integrità e disponibilità** delle informazioni gestite;
- la **trasparenza verso cittadini e istituzioni**;
- la **conformità agli obblighi di notifica e comunicazione** previsti dalla legge.

Il Piano fornisce **alle Direzioni, ai Settori e alle strutture di supporto agli organi di direzione politico-amministrativa della Regione Piemonte,** un quadro di riferimento univoco per la gestione degli incidenti, favorendo la cooperazione tra le strutture tecniche, legali e direzionali nella prevenzione, risposta e comunicazione degli eventi di sicurezza.

Il **Coordinamento Direttori** approva il presente piano e ne garantisce l'effettiva attuazione attraverso le strutture regionali, mantenendo un costante rapporto con il Referente per la Cybersicurezza.[1] La **Giunta Regionale** autorizza l'adozione del piano stesso.

CAMPO DI APPLICAZIONE

Il presente piano si applica a:

- Tutti i **Settori** e le **Direzioni** della Regione Piemonte;
- i **dipendenti, collaboratori e consulenti** che trattano dati, informazioni o servizi ICT;
- i **fornitori di servizi esterni**, qualora gestiscano sistemi, dati o componenti infrastrutturali o applicative;
- le **amministrazioni** che utilizzano servizi messi a disposizione dalla Regione Piemonte, per le attività di prevenzione, rilevazione e gestione condivisa degli incidenti informatici.

Sono esclusi dal perimetro solo gli eventi non riconducibili alla sicurezza delle informazioni o che riguardano esclusivamente il malfunzionamento tecnico di apparati non connessi a dati o servizi dell'Ente.
Il piano si applica congiuntamente alla procedura di **Gestione incidenti di sicurezza IT**, che ne costituisce il livello operativo di dettaglio.

[1] Requisito NIS2 RS.MA-01 punto 2

Il presente piano è riesaminato e, se opportuno, aggiornato periodicamente e comunque almeno ogni due anni[2], o qualora si presentino:

- incidenti significativi, integrando le relative lezioni apprese, o mutamenti dell'esposizione alle minacce e ai relativi rischi.
- aggiornamenti normativi o regolamentari di rilievo con impatto sulla cybersecurity;
- modifiche sostanziali all'assetto organizzativo o tecnologico dell'Ente;
- evidenze di non conformità emerse da audit interni o esterni;
- raccomandazioni del Referente per la Cybersicurezza e/o del Coordinamento Direttori;

GLOSSARIO E RIFERIMENTI INTERNI

1.1 GLOSSARIO DEI TERMINI

TERMINE	DEFINIZIONE SINTETICA
Evento di sicurezza	Qualsiasi anomalia, comportamento inatteso o situazione che possa compromettere la sicurezza delle informazioni, dei sistemi o delle reti della Regione Piemonte. Gli eventi possono non causare danni effettivi ma rappresentare segnali di potenziale rischio.
Incidente di sicurezza IT	Evento o insieme di eventi che provocano o possono provocare un impatto negativo sulla riservatezza, integrità o disponibilità delle informazioni o dei servizi IT della Regione Piemonte. Comprende anche gli incidenti infrastrutturali e i casi di data breach.
Data Breach	Violazione di dati personali che comporta distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trattati dalle Regione Piemonte o dai suoi fornitori, come definito dal Regolamento (UE) 2016/679 (GDPR).
Notifica	Comunicazione formale di un incidente alle autorità competenti (ACN, CSIRT Italia, Garante Privacy) entro le tempistiche stabilite dalla normativa.
Segnalazione	Comunicazione interna iniziale di un evento o incidente da parte di un dipendente, collaboratore o fornitore ai canali designati (es. Responsabile della Sicurezza IT o suo sostituto, punto di contatto CSIRT o suo sostituto).
Referente per la Cybersicurezza	Coordina la gestione degli incidenti, garantisce la conformità normativa e rappresenta il punto di contatto ufficiale verso ACN e CSIRT Nazionale.
SOC – Security Operations Center	Struttura organizzativa competente in ambito sicurezza che opera per il monitoraggio, l'analisi e la risposta agli incidenti di sicurezza informatica.
CSIRT Italia	Struttura nazionale, interna ad ACN, responsabile della prevenzione, gestione e risposta agli incidenti di sicurezza informatica che coinvolgono infrastrutture critiche, pubbliche amministrazioni, operatori di servizi essenziali e soggetti rilevanti per la sicurezza del Paese. Coordina attività di monitoraggio, analisi delle minacce, gestione degli incidenti e condivisione tempestiva di informazioni di sicurezza.
ACN – Agenzia per la Cybersicurezza Nazionale	Autorità nazionale responsabile del coordinamento e della gestione della cybersicurezza a livello statale. Riceve le notifiche di incidente e coordina la risposta a livello nazionale.
PCO – Piano di Continuità Operativa	Documento interno che definisce le misure e le strategie per garantire la continuità dei servizi critici in caso di incidenti o interruzioni significative.

[2] Requisito NIS2 RS.MA-01 punto 3

TERMINE	DEFINIZIONE SINTETICA
Need to Know	Principio di sicurezza secondo cui l'accesso a informazioni, sistemi o risorse è concesso solo agli individui che ne hanno un reale e comprovato bisogno per svolgere le proprie attività lavorative. L'obiettivo è ridurre l'esposizione dei dati sensibili limitando la superficie di attacco e prevenendo accessi non autorizzati, intenzionali o accidentali.
Attacco DDoS	Attacco informatico in cui un elevato numero di sistemi compromessi (botnet) invia simultaneamente grandi quantità di traffico verso un servizio, un server o una rete, con l'obiettivo di saturarne le risorse e renderlo non disponibile agli utenti fruitori. L'attacco sfrutta la distribuzione geografica e numerica delle fonti per rendere difficile l'identificazione e il filtraggio del traffico malevolo.
Attacco ransomware	Tipologia di attacco informatico in cui un malware cifra i dati o blocca i sistemi di un'organizzazione, rendendoli inaccessibili. Gli attaccanti richiedono poi un riscatto (ransom) per fornire la chiave di decrittazione o per evitare la pubblicazione dei dati sottratti.
SLA, OLA	**SLA**: Accordo formale tra un fornitore di servizi e un cliente che definisce i livelli di servizio attesi, gli indicatori di qualità (KPI), i tempi di risposta e ripristino, le responsabilità delle parti e le modalità di monitoraggio. Lo SLA stabilisce in modo misurabile che cosa deve essere garantito e a quali condizioni. **OLA**: Accordo interno tra diverse unità operative della stessa organizzazione che definisce responsabilità, tempi e attività necessarie per supportare il rispetto degli SLA verso il cliente finale.

RIFERIMENTI TECNICI E ORGANIZZATIVI

- **ISO/IEC 27035:2023** – *Information Security Incident Management*;
- **ISO/IEC 27001:2022** – *Information Security Management Systems*;
- **Strategia Nazionale di Cybersicurezza 2022–2026**, promossa da ACN;
- **Procedure operative della Regione Piemonte** e procedure correlate (*Gestione Incidenti, Piano di Continuità Operativa*).
- **Legge 90/2024** – Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.
- **Dlgs 138/2024** – Decreto Legislativo e regolamenti associati per l'adozione della Direttiva NIS2.
- **Dgr n. 1-7574** del 28/09/2018 - Adempimenti in attuazione al Regolamento UE 2016/679. Designazione degli incaricati e istruzioni operative. Disposizioni procedurali in materia di incidenti di sicurezza e di violazione di dati personali (Data Breach), adozione del relativo registro e modello di informativa.
- **Guida alla notifica degli incidenti al CSIRT Italia**

L'applicazione di tali riferimenti assicura che la gestione degli incidenti di sicurezza IT della Regione Piemonte sia coerente con i requisiti di legge, con le linee guida dell'Agenzia per la Cybersicurezza Nazionale e con le migliori pratiche internazionali in materia di sicurezza delle informazioni.

1.2 RIFERIMENTI INTERNI

TITOLO	DESCRIZIONE SINTETICA
Piano di Gestione degli incidenti di sicurezza	Definisce il piano generale di gestione degli incidenti di sicurezza IT.
Procedura di Gestione degli Incidenti di Sicurezza IT	Descrive le modalità operative per la rilevazione, classificazione, analisi e risoluzione degli incidenti informatici.
Piano di Continuità Operativa	Definisce le strategie per garantire la disponibilità dei servizi critici in caso di emergenze o incidenti di sicurezza.
Registro degli incidenti di sicurezza	Registro che raccoglie e traccia tutti gli incidenti registrati, la loro classificazione e le azioni di follow-up.

PRINCIPI DI GESTIONE E POLITICHE

La Regione Piemonte adotta un modello unificato di **gestione degli incidenti di sicurezza IT** basato su principi di tempestività, trasparenza, responsabilità e miglioramento continuo.

Il modello si fonda sui seguenti **principi di governance**:

- **Centralità della gestione coordinata**
  Tutti gli incidenti di sicurezza IT sono gestiti attraverso un processo integrato che coinvolge le funzioni tecniche, organizzative e direzionali sotto la supervisione del **Responsabile della Sicurezza IT**.
- **Accountability e responsabilità condivisa**
  Ogni funzione organizzativa è tenuta a cooperare con il Referente per la Cybersicurezza e con il Gruppo di Lavoro Cybersicurezza, già costituito con DD 11/A1000A del 22/01/2025, segnalando tempestivamente ogni evento potenzialmente riconducibile a un incidente di sicurezza.
- **Tempestività e obblighi di notifica**
  In caso di **incidenti significativi**, la Regione Piemonte è tenuta alla notifica verso lo **CSIRT Italia (ACN)** secondo procedure e tempistiche prestabilite. La gestione degli incidenti deve prevedere, secondo la normativa vigente, una prima comunicazione, volta a fornire un avviso tempestivo e, se possibile, indicazioni preliminari sull'eventuale natura malevola dell'incidente o sul suo possibile impatto transfrontaliero. Successivamente deve essere inviata una notifica completa, aggiornata e contenente una valutazione iniziale della gravità e dell'impatto, nonché eventuali indicatori di compromissione. Durante tutto il ciclo di gestione dell'incidente possono essere predisposte relazioni intermedie su richiesta dello CSIRT Italia, mentre deve essere predisposta una la relazione finale, trasmessa entro i termini stabiliti, che descrive in dettaglio l'incidente, le cause o le minacce all'origine, le misure di contenimento adottate e l'evoluzione della situazione fino alla sua conclusione. Tutte le comunicazioni devono essere effettuate tempestivamente e secondo quanto previsto dalla normativa vigente, garantendo al CSIRT Italia una completa e corretta informazione.
- **Principio del "need-to-know" e riservatezza delle informazioni**
  Le informazioni relative agli incidenti sono condivise esclusivamente con i soggetti autorizzati e nel rispetto dei vincoli di riservatezza, integrità e protezione dei dati personali.
- **Integrazione con la continuità operativa e la gestione del rischio**
  La gestione degli incidenti di sicurezza IT è coordinata con il **Piano di Continuità Operativa** e con il processo di **Risk Management** dell'organizzazione, al fine di garantire la resilienza dei servizi essenziali per l'Ente.

- **Analisi e miglioramento continuo**
  Ogni incidente significativo è oggetto di una revisione post-evento ("*lessons learned*") finalizzata a individuare azioni preventive, aggiornare le procedure e migliorare le misure tecniche e organizzative.
- **Cultura della sicurezza e formazione**
  Regione Piemonte promuove la consapevolezza e la formazione continua del personale e dei fornitori, affinché ogni soggetto sia in grado di riconoscere, segnalare e gestire correttamente un potenziale incidente.

Corresponsabilità organizzativa

La gestione degli incidenti di sicurezza IT è una **responsabilità estesa.** Ogni struttura della Regione Piemonte, indipendentemente dal proprio ruolo tecnico, amministrativo o gestionale, contribuisce attivamente alla prevenzione, alla segnalazione e alla corretta comunicazione degli incidenti.

RUOLI E RESPONSABILITÀ

Il modello di **gestione degli incidenti di sicurezza** della Regione Piemonte si basa su una governance multilivello, che assicura la responsabilità diretta degli organi di vertice e una chiara distinzione tra ruoli decisionali, di coordinamento e operativi.
I ruoli coinvolti sono definiti nel documento "Modello di Organizzazione della sicurezza adottato dalla Regione Piemonte; qui di seguito si riprende la tabella riepilogativa riferita ai soli ruoli rientranti nel processo di gestione degli incidenti di sicurezza:

Ruolo	Responsabilità
Coordinamento Direttori	Governare il sistema di gestione dei rischi (strategici e operativi). Coordinare le iniziative in materia di sicurezza fisica, ICT e protezione dei dati personali, contribuendo a definire strategie e policy aziendali e garantendone l'applicazione nell'attività di progettazione e gestione di applicazioni e Infrastrutture, nonché nella gestione della sicurezza delle sedi, delle persone e dei dati Governare la Business Continuity, contribuendo alla definizione di strategie e policy aziendali atte a migliorare la resilienza tecnico-organizzativa del Consorzio rispetto a situazioni di crisi che possano inficiare sulla continuità operativa dei servizi erogati Affrontare e dirimere problematiche connesse alla sicurezza ICT, sicurezza fisica, continuità operativa e protezione dei dati, compresa la gestione degli incident e dei change tecnico-organizzativi che hanno impatti su tali ambiti.
Referente per la Cybersicurezza	Definire la strategia di sicurezza informatica dell'azienda; garantire la conformità alle normative di settore (es. normativa NIS2); supervisionare le attività di gestione del rischio, incident response e formazione.
Responsabile Security Operations Center - SOC	Monitorare la sicurezza dei sistemi e servizi della Regione Piemonte; prevenzione, rilevamento, analisi e risposta agli eventi di sicurezza; supporto all'implementazione delle misure tecniche.
Unità di crisi	L'Unità di crisi è definita in funzione dello scenario che si verifica e della materia di riferimento. Coordina e gestisce la risposta aziendale in caso di incidente.

DPO – Data Protection Officer (Responsabile della protezione dei dati)	Coordinare le politiche di sicurezza con il GDPR e i requisiti NIS2, supportando la notifica degli incidenti, collaborare con i team di sicurezza per la conformità e la formazione del personale.
Settore competente Privacy	Supporta le strutture organizzative nell'attuazione degli adempimenti in materia di protezione dei dati personali.
Punto di contatto NIS2[3] *ex D.Lgs. 138/2024 – Art.7 co.1, lett c)*	Effettuare la registrazione sulla piattaforma ACN, la gestione e l'aggiornamento dei dati, il coordinamento delle notifiche di incidenti di sicurezza e il monitoraggio delle misure adottate dall'Ente.
Sostituto punto di contatto NIS2[3] *ex D.Lgs. 138/2024 – Art.7 co.4, lett d)*	In caso di assenza del punto di contatto effettuare, la gestione e l'aggiornamento dei dati, il coordinamento delle notifiche di incidenti di sicurezza e il monitoraggio delle misure adottate dall'azienda.
Referente CSIRT[4] **e suo/i sostituto/i** *(da nominare)*	Interloquisce con lo CSIRT Italia ed effettuare le notifiche di cui agli articoli 25 e 26 del D.Lgs. 138/2024 per conto del soggetto NIS.
Referenti Privacy di Direzione	In caso di incidenti che contemplano la perdita di sicurezza di dati personali, sono figure che, rispettivamente per ogni Direzione, forniscono supporto alle segnalazioni, come da DGR n. 1-7574 del 28/09/2018.

GESTIONE, COMUNICAZIONE E NOTIFICA DEGLI INCIDENTI

La Regione Piemonte adotta un processo di **gestione e comunicazione strutturata** degli incidenti di sicurezza informatica, in conformità con le disposizioni della **Legge 90/2024**, della **Direttiva NIS2** e delle procedure interne.
L'obiettivo è garantire che tutte le informazioni rilevanti siano comunicate ai soggetti competenti, interni ed esterni, in modo **tracciabile, sicuro e coerente** con i principi di riservatezza e trasparenza istituzionale.

1.3 PROCESSO DI GESTIONE DEGLI INCIDENTI DI SICUREZZA[5]

Il processo di gestione degli incidenti di sicurezza, in conformità alla Legge 90/2024 e al D.Lgs. 138/2024 (NIS2), costituisce un pilastro fondamentale per la resilienza operativa e la protezione dei dati aziendali. Tale processo è strutturato per garantire rapidità di intervento, tracciabilità delle azioni e conformità normativa, attraverso fasi integrate e coordinate sotto la supervisione del Responsabile della Sicurezza IT, con il coinvolgimento del SOC, delle strutture organizzative interne o esterne che possono fornire supporto o competenza nella gestione degli incidenti.
L'obiettivo principale è assicurare che ogni incidente venga gestito in modo strutturato, riducendo al minimo l'impatto su servizi critici e dati sensibili, e rispettando gli obblighi di notifica previsti dalla normativa nazionale ed europea. Il processo si articola nelle seguenti macro-fasi. Il processo di gestione degli incidenti è articolato secondo una procedura operativa di dettaglio definita e aggiornata periodicamente dal Settore Sistema Informativo Regionale, in collaborazione con Settore Servizi Infrastrutturali e Tecnologici.

La gestione degli incidenti di sicurezza IT di Regione Piemonte è conforme alle **linee guida emanate da ACN.**

[3] Determinazione ACN 164179 del 14 aprile 2025 – Allegato 2. Requisito GV.RR.02 – Punto 3
[4] Determinazione ACN 333017/2025
[5] Requisito NIS2 RS.MA-01 punto 1c

1.4 FUNZIONI DA CUI PUÒ PERVENIRE LA SEGNALAZIONE DI UN INCIDENTE

Chiunque identifichi l'accadimento di un evento di sicurezza informatico o di una presumibile violazione della riservatezza, integrità o disponibilità dei dati gestiti dalle Regione è tenuto a darne tempestiva comunicazione. I canali di segnalazione sono di massima così identificati:

- Il Settore Sistema Informativo Regionale e Settore Servizi Infrastrutturali e Tecnologici, nonché il Gruppo di Lavoro Cybersicurezza
- le singole strutture organizzative della Regione Piemonte
- le strutture organizzative della Regione a fronte di segnalazione diretta di utenti o di segnalazione esterna, che si cataloghi come possibile rischio di sicurezza delle informazioni
- Il Settore Patrimonio immobiliare, beni mobili, economato, cassa economale e sicurezza ambienti di lavoro e il Settore Gestione e Sicurezza Palazzo Unico, in quanto competenti per la sorveglianza incidenti sulla consistenza fisica degli asset (ad es. casi di furto, danneggiamento, eventi dolosi o interruzioni dell'alimentazione elettrica, ecc.…)
- soggetti esterni all'azienda quali Polizia Postale, Pubblica Amministrazione centrale (ad es. CSIRT Italia)
- il SOC (Security Operation Center), presso CSI Piemonte, che nota anomalie a seguito dell'analisi di log/traffico sull'infrastruttura o di altri monitoraggi.

1.4.1 Rilevazione e Segnalazione

Questa fase prevede il monitoraggio continuo degli asset e dei sistemi, l'analisi degli alert provenienti da strumenti di sicurezza e la segnalazione tempestiva di anomalie ai gruppi tecnici competenti. Tutti i dipendenti hanno l'obbligo di comunicare eventi sospetti secondo le policy interne.

Informazioni di contatto per la segnalazione di incidenti: [6]

Le segnalazioni di incidenti di sicurezza vanno indirizzate tempestivamente, non appena se ne è avuta conoscenza, al Referente per la Cybersicurezza, al Settore Sistema Informativo Regionale e al Settore Servizi Infrastrutturali e tecnologici, all'indirizzo mail: notifica.incidenti.sicurezzainformatica@regione.piemonte.it.

Ulteriori dettagli sul processo sono rimandati alla procedura di gestione degli incidenti di sicurezza.

1.4.2 Classificazione e Analisi

L'incidente viene classificato in base alla gravità, alla tipologia (es. attacco DDoS, attacco ransomware, compromissione di account) e all'impatto su dati e servizi. Il Referente per la Cybersicurezza coordina la raccolta delle evidenze e la valutazione preliminare, coinvolgendo eventualmente il DPO in caso di impatto su dati personali.

[6] Requisito NIS2 RC.RP-01 punto 1

1.4.3 Contenimento e Mitigazione

Prevede l'attivazione di misure tecniche e organizzative per limitare la propagazione dell'incidente e ridurre l'impatto. Le azioni possono includere, ad esempio, l'isolamento di sistemi compromessi, il blocco di account, l'applicazione di patch di sicurezza, la revoca di account o privilegi utente.

1.4.4 Comunicazione e Notifica

Prevede la gestione delle comunicazioni interne ed esterne, inclusa la notifica obbligatoria allo CSIRT Italia entro le tempistiche di legge. In caso di data breach, si applicano anche le disposizioni del GDPR; si rimanda per i dettagli alla procedura di gestione dei data breach.

Si rimanda al par. 1.7 per la descrizione dettagliata del processo di comunicazione.

1.4.5 Risoluzione, Ripristino e Chiusura

Prevede il ripristino dei servizi e la normalizzazione degli ambienti impattati al fine di riprendere la normale operatività. Questa fase può includere attività di digital forensics per individuare le cause e raccogliere prove utili ai fini delle comunicazioni alle Autorità. Ripristinati i servizi viene gestita la comunicazione di chiusura dell'incidente verso tutti i soggetti coinvolti e/o impattati.

Le procedure per il ripristino dei sistemi, sono documentate nell'ambito del Piano di Continuità Operativa PCO[7].

1.4.6 Reporting e Miglioramento Continuo

Prevede la redazione della documentazione completa dell'incidente, l'analisi delle cause radice e la definizione di azioni correttive. Le lezioni apprese vengono integrate nel piano di sicurezza e nelle procedure operative, secondo il metodo PDCA (Plan-Do-Check-Act).

Questo metodo di gestione e miglioramento continuo basato su quattro fasi iterative: pianificare, attuare, verificare e agire è utilizzato per strutturare processi organizzativi, valutare l'efficacia dei controlli e introdurre miglioramenti costanti.

Le fasi principali del ciclo sono:
- Plan (Pianificare): definire obiettivi, requisiti, rischi e azioni necessarie.
- Do (Fare): implementare le attività pianificate e applicare i controlli previsti.
- Check (Verificare): monitorare i risultati, misurare le prestazioni e valutare eventuali scostamenti.
- Act (Agire): adottare azioni correttive e migliorative per ottimizzare il processo.

[7] Requisito NIS2 DE.CM-01 punto 2

1.4.7 Matrice RACI – Ruoli e Responsabilità

Fase	Responsabile (R)	Accountable (A)	Consulted (C)	Informed (I)
Rilevazione e Segnalazione	Team SOC, CSIRT Regione Piemonte, fornitori servizi ICT	Referente per la Cybersicurezza	Settore Sistema Informativo Regionale, Settore Servizi Infrastrutturali e Tecnologici, DPO, Referenti Privacy	Utenti regionali
Classificazione e Analisi	Referente CSIRT o suo sostituto	Referente per la Cybersicurezza	SOC, Settore Sistema Informativo Regionale, Settore Servizi Infrastrutturali e Tecnologici, DPO, Referenti Privacy	Strutture organizzative coinvolte
Contenimento e Mitigazione	SOC e fornitori servizi ICT	Referente per la Cybersicurezza	Settore Sistema Informativo Regionale, Settore Servizi Infrastrutturali e Tecnologici, DPO	Coordinamento Direttori, soggetti impattati
Comunicazione e Notifica	Referente CSIRT o suo sostituto	Referente per la Cybersicurezza	Capo di Gabinetto, Portavoce del Presidente, Direttore competente per la comunicazione istituzionale, DPO	Autorità, Stakeholder, Referenti Privacy
Risoluzione e Ripristino	SOC e fornitori servizi ICT	Referente per la Cybersicurezza	Settore Sistema Informativo Regionale, Settore Servizi Infrastrutturali e Tecnologici, Referente CSIRT	Coordinamento Direttori
Reporting e Miglioramento	Referente CSIRT	Referente per la Cybersicurezza	Settore Sistema Informativo Regionale, Settore Servizi Infrastrutturali e	Coordinamento Direttori

			Tecnologici	

Nel caso l'incidente di sicurezza rientri nel perimetro definito della DGR n. 1-7574 del 28/09/2018, fare riferimento alla rispettiva RACI, parte integrante del medesimo documento.

1.5 INCIDENTI SIGNIFICATIVI PER CUI È RICHIESTA LA NOTIFICA

Secondo la tassonomia di cui all'articolo 25, comma 4, del D.lgs. 138/2024, si definisce significativo un incidente che:

A. ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
B. ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Le specifiche ACN, rispetto agli incidenti significativi per i "soggetti importanti", classifica gli incidenti significativi in queste tre macrocategorie:

- **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;

In riferimento alla categoria IS-3 i livelli di servizio atteso (SL) sono definiti negli SLA contrattuali con i singoli fornitori e declinati nel piano di Continuità Operativa Integrato (PCO).[8]

1.6 NOTIFICA VERSO AUTORITÀ E ORGANISMI NAZIONALI[9]

Regione Piemonte, in quanto soggetto classificato da ACN come "importante", è tenuto alla **notifica obbligatoria** degli incidenti di sicurezza informatica secondo quanto previsto dalla **Legge 90/2024** e dalla **Direttiva (UE) 2022/2555 (NIS2)**. In caso di incidenti significativi è obbligato ad effettuare la notifica allo CSIRT Italia (ACN) secondo le modalità e tempistiche di seguito riportate:

- senza ingiustificato ritardo, e **comunque entro 24 ore** da quando è venuto a conoscenza dell'incidente significativo, effettua l'invio di una pre-notifica che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

[8] Requisito NIS2 RS.MA-01 punto 1e
[9] Requisito NIS2 RS.CO-02 punto 1

- senza ingiustificato ritardo, e **comunque entro 72 ore** da quando è venuto a conoscenza dell'incidente significativo, effettua l'invio di una notifica dell'incidente che, ove possibile, aggiorni le informazioni di cui al punto precedente e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
- su richiesta della CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;
- una relazione finale **entro un mese** dalla trasmissione della notifica dell'incidente di cui al punto precedente, che comprenda:
    1. una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;
    2. il tipo di minaccia o la causa originale che ha determinato lo sviluppo dell'incidente;
    3. le misure di contenimento adottate e in corso;
- in caso di incidente in corso al momento della trasmissione della relazione finale di cui al punto precedente, una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

- contestualmente, la valutazione della necessità di comunicazione verso le strutture regionali, enti che usufruiscono di servizi regionali e altre autorità competenti.

- in caso di incidenti che coinvolgono dati personali, **il Titolare del trattamento** provvede alla notifica al Garante per la protezione dei dati personali, secondo le tempistiche previste dal Regolamento (UE) 2016/679 (GDPR) e attraverso le procedure definite dall'Ente, **sentito il DPO (RPD)**, come previsto dalla **DGR n. 1-7574** del 28 settembre 2018.

In caso di incidenti significativi, le notifiche e le relazioni sono predisposte dalla struttura organizzativa preposta al governo della cybersicurezza, in collaborazione con le strutture organizzative aziendali coinvolte ed inviate dal Referente per la Cybersicurezza o suo sostituto (punto di contatto, referente CSIRT, e rispettivi sostituti), come previsto dal modello organizzativo dell'Ente che provvede a trasmetterle allo CSIRT Italia e/o alle Autorità.
I modelli di reportistica da utilizzare sono definiti e aggiornati dal Referente per la Cybersicurezza, dal Settore Sistema Informativo Regionale e dal Settore Servizi Infrastrutturali e tecnologici,[10] e costituiscono un allegato della procedura di gestione degli incidenti di sicurezza.

1.7 COMUNICAZIONE VERSO STRUTTURE INTERNE INTERESSATE, ARTICOLAZIONI COMPETENTI, ENTI FRUITORI E ISTITUZIONI[11]

In presenza di incidenti di sicurezza con impatti sui servizi propri o erogati a enti terzi, la Regione Piemonte, attraverso le funzioni delegate alla gestione della comunicazione interna ed esterna:

- Informa tempestivamente le strutture organizzative interessate, le articolazioni competenti (Referente per la Cybersicurezza, SOC, CSIRT Regionale ecc.);
- informa tempestivamente i referenti designati dell'ente, secondo le modalità previste dai contratti di servizio (SLA, OLA);

[10] Requisito NIS2 RS.CO-02 punto 2

[11] Requisiti NIS2 RC.CO-03 punto 1 e RS.MA-01 punto 1d

- assicura la trasparenza delle informazioni, comunicando lo stato dell'incidente, le misure correttive intraprese, le attività e le tempistiche di ripristino;
- mantiene la riservatezza dei dati e delle informazioni tecniche, condividendo solo quanto necessario alla gestione coordinata dell'emergenza.

Il processo di comunicazione è rivolto inoltre[12]:

- ai fruitori dei servizi impattati da incidenti di sicurezza che possono avere impatti in termini di fruizione (riservatezza, disponibilità e/o integrità dei dati)
- ai destinatari di servizi potenzialmente interessati da una minaccia informatica significativa ai quali vanno indicate misure o azioni correttive o di mitigazione che possono essere adottate al fine al fine di mitigare il rischio di incidente.
- Ai fornitori di servizio che fanno parte della catena di fornitura dell'Ente qualora vengano rilevate minacce che dipendono da questi ultimi (es. vulnerabilità, sistemi o utenze compromesse, etc..) e che possano ripercuotersi negativamente sui servizi erogati.

Le comunicazioni interne avvengono secondo processi e strumenti attuati secondo quanto definito dall'organizzazione regionale.
Le comunicazioni esterne avvengono esclusivamente tramite i canali gestiti dalla Regione Piemonte, per garantire coerenza istituzionale e prevenire la diffusione non autorizzata di informazioni sensibili.

1.7.1 Comunicazione interna[13]

La segnalazione di un potenziale incidente può essere effettuata da qualsiasi dipendente, collaboratore o fornitore della Regione Piemonte attraverso i canali previsti dalle procedure operative.
Le comunicazioni interne seguono il principio del **need-to-know** e sono indirizzate:

- al **Referente per la Cybersicurezza**, quale referente centrale per la gestione dell'incidente;
- al **SOC**, per la valutazione tecnica e l'analisi preliminare;
- al **Coordinamento Direttori**, nel caso di incidenti con impatto significativo o potenziale di propagazione.

Il Responsabile della Sicurezza IT valuta la classificazione dell'incidente e coordina la comunicazione verso i soggetti interni competenti secondo le modalità e i tempi previsti dalla normativa.

1.7.2 Comunicazione pubblica e relazioni esterne

Nel caso di incidenti di particolare rilevanza pubblica o potenziale impatto reputazionale, l'Ufficio del Gabinetto del Presidente della Giunta Regionale, il Portavoce del Presidente, il Direttore competente per la comunicazione istituzionale, in collaborazione con gli uffici di comunicazione interessati in relazione all'incidente verificatosi e in raccordo con il Referente per la Cybersicurezza, definiscono le modalità e i contenuti delle comunicazioni esterne, nel rispetto delle normative sulla trasparenza e sulla sicurezza nazionale.

[12] Requisito NIS2 RS.MA-01 punto 1a

[13] Requisito NIS2 RS.MA-01 punto 1b

Nel caso in cui l'Agenzia per la Cybersicurezza Nazionale (ACN), ai sensi dell'art. 37, comma 3, lettera i) del decreto NIS, intimasse all'organizzazione di informare il pubblico riguardo a un incidente informatico, quest'ultima adotta un processo strutturato per garantire una comunicazione tempestiva, trasparente e coerente[14].

La ricezione dell'intimazione da parte dell'ACN attiva tempestivamente il Comitato di crisi, come previsto dal Piano di Continuità Operativa (PCO). Questo gruppo ha il compito di raccogliere le informazioni necessarie e predisporre un comunicato ufficiale da diffondere al pubblico.

Il comunicato viene redatto seguendo alcuni principi fondamentali:

- Trasparenza, per assicurare che le informazioni siano accurate e comprensibili;
- Tempestività, per rispettare le scadenze indicate dall'ACN;
- Coerenza, affinché i messaggi diffusi attraverso i diversi canali (sito web, social media, comunicati stampa) siano uniformi;
- Tutela, per evitare la divulgazione di dati sensibili o di dettagli tecnici che possano compromettere ulteriormente la sicurezza.

Il testo del comunicato contiene una descrizione sintetica dell'incidente, l'indicazione dell'impatto sugli utenti o cittadini, le misure adottate per mitigare le conseguenze e, ove necessario, istruzioni pratiche per ridurre i rischi (ad esempio, modificare le credenziali o prestare attenzione a possibili campagne di phishing).

1.8 TRACCIABILITÀ E RISERVATEZZA

Tutte le comunicazioni e notifiche relative agli incidenti di sicurezza IT sono **tracciate e archiviate** in modo sicuro, nel rispetto delle politiche di conservazione dei dati e della documentazione dell'Ente. L'accesso alle informazioni è limitato ai soli soggetti autorizzati, nel rispetto del principio di **minimizzazione** e dei requisiti di **integrità e riservatezza** delle informazioni.

REPORTING E RIESAME

Il Settore Sistema Informativo Regionale, in collaborazione con il Settore Servizi Infrastrutturali e Tecnologici, adotta un sistema strutturato di **reporting e riesame** finalizzato a garantire al **Coordinamento Direttori** e alla **Giunta Regionale** una visione costante sul livello di sicurezza informatica e sull'efficacia del modello di gestione degli incidenti.
Il **Referente per la Cybersicurezza** è responsabile della predisposizione dei report periodici e della loro presentazione agli organi di governo e di controllo.

1.9 REPORTING PERIODICO AL COORDINAMENTO DIRETTORI

Il Referente per la Cybersicurezza, unitamente al Business Continuity e Risk manager, relazionano periodicamente (2 volte l'anno) al Coordinamento Direttori, presentando informazioni relative all'ambito di sicurezza, (gestione incidenti, validazione procedure, informazioni di prevenzione, etc..).

[14] Requisito NIS2 RS.MA-01 punto 1d

Il **Referente per la Cybersicurezza** redige con cadenza almeno **semestrale** un **Rapporto riepilogativo sulla Gestione degli Incidenti di Sicurezza IT**, contenente:

- il numero complessivo degli incidenti rilevati e classificati per tipologia e criticità;
- i tempi medi di gestione;
- le principali cause radice (*root cause analysis*) e le azioni correttive adottate;
- eventuali criticità sistemiche o rischi emergenti.

Il **Coordinamento Direttori** analizza il rapporto, valuta l'efficacia delle misure adottate e propone eventuali azioni di miglioramento o risorse necessarie per far fronte alla gestione dei rischi cyber.

MIGLIORAMENTO CONTINUO

Regione Piemonte persegue un approccio di **miglioramento continuo** della gestione degli incidenti di sicurezza IT, attraverso:

- l'analisi sistematica delle cause e delle vulnerabilità riscontrate;
- la definizione e il monitoraggio di **indicatori di performance (KPI)** e la valutazione di efficacia delle misure adottate;
- la promozione di programmi di formazione, esercitazioni e simulazioni di incidenti (*tabletop exercise*);
- l'adozione di tecnologie e pratiche avanzate di monitoraggio, detection e risposta;
- la revisione periodica delle procedure operative (**Procedura Gestione Incidenti**) in coerenza con gli aggiornamenti normativi e tecnologici.

1.10 DIFFUSIONE E CONSAPEVOLEZZA

Il Piano di gestione degli incidenti di sicurezza è pubblicato sul portale intranet della Regione Piemonte e reso disponibile a tutto il personale e ai soggetti interessati.
Il **Settore Sviluppo e Capitale Umano**, in collaborazione con il **Referente per la Cybersicurezza, con il Settore Sistema Informativo Regionale e con il Settore Servizi Infrastrutturali e Tecnologici,** assicura la diffusione delle informazioni e la promozione di una **cultura aziendale della sicurezza**, affinché tutti i soggetti coinvolti comprendano il proprio ruolo nella prevenzione e gestione degli incidenti informatici.

VERIFICHE ED APPROVAZIONI

VER.	REDAZIONE		CONTROLLO ED APPROVAZIONE		AUTORIZZAZIONE ALL'EMISSIONE	
	NOME	DATA	NOME	DATA	NOME	DATA
V01						

STATO DELLE VARIAZIONI

VER.	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
V01	Tutto il documento	Prima versione del documento

INDICE

.....1

1 SCOPO E CAMPO DI APPLICAZIONE.....3

1.1 CONTESTO STRATEGICO.....3
1.2 OBIETTIVO.....3
1.3 CAMPO DI APPLICAZIONE.....3

2 RIFERIMENTI.....4

2.1 NORMATIVA VIGENTE.....4
2.2 RIFERIMENTI TECNICI.....4
2.3 RIFERIMENTI DOCUMENTALI.....4

3 GLOSSARIO.....5

3.1 GLOSSARIO DEI TERMINI.....5
3.2 ACRONIMI.....6

4 PRINCIPI.....6

4.1 PREVENZIONE E TEMPESTIVITÀ.....6
4.2 ACCOUNTABILITY E OWNERSHIP.....7
4.3 PROPORZIONALITÀ E APPROCCIO RISK-BASED.....7
4.4 CONFORMITÀ BY DESIGN.....7
4.5 MIGLIORAMENTO CONTINUO.....7

5 GOVERNANCE E RESPONSABILITÀ.....7

5.1 MODELLO ORGANIZZATIVO.....7
5.2 RUOLI E RESPONSABILITÀ (TABELLA RACI).....7
5.3 DESCRIZIONE DEI RUOLI.....8

6 REQUISITI DI CONFORMITÀ E OBBLIGHI NORMATIVI.....9

6.1 OBBLIGHI NORMATIVI.....9
6.2 CLASSIFICAZIONE E CRITERI DI GESTIONE DELLE TEMPISTICHE.....9
6.3 PRESIDI DI SICUREZZA NEL CICLO DI VITA DEI SISTEMI, DEI SERVIZI ICT E DEI RAPPORTI CON I FORNITORI.....10

7 PROCESSI.....10

7.1 GESTIONE DELLE FONTI INFORMATIVE E DELLE INFORMAZIONI SUI SISTEMI E COMPONENTI MONITORATI.....11
7.2 PRESA IN CARICO, VERIFICA DI APPLICABILITÀ E TRATTAMENTO DELLE VULNERABILITÀ.....11
7.3 GESTIONE DELLE SEGNALAZIONI ESTERNE DI VULNERABILITÀ.....13

8 REPORTING, RIESAME ED ESCALATION.....14

8.1 REPORTING PERIODICO E RIESAME DIREZIONALE.....14
8.2 COMUNICAZIONI STRAORDINARIE ED ESCALATION.....14

9 MIGLIORAMENTO CONTINUO.....15

9.1 DIFFUSIONE E CONSAPEVOLEZZA.....15

1 SCOPO E CAMPO DI APPLICAZIONE

Il presente Piano definisce l'approccio della Regione Piemonte alla gestione delle vulnerabilità di sicurezza informatica, in coerenza con la direttiva (UE) 2022/2555, con il decreto legislativo 4 settembre 2024, n. 138, con la legge 28 giugno 2024, n. 90, con il decreto legislativo 7 marzo 2005, n. 82 e con gli atti organizzativi regionali adottati in materia di cybersicurezza. Esso disciplina, a livello organizzativo, i principi, le responsabilità e il quadro generale di riferimento per l'identificazione, la valutazione, il trattamento e il monitoraggio delle vulnerabilità che possono incidere sulla sicurezza dei sistemi informativi e di rete e sulla continuità dei servizi digitali regionali.
Il Piano si inserisce nell'impianto documentale della sicurezza informatica della Regione Piemonte ed è coordinato con il REGP_POL01 – Organizzazione per la sicurezza informatica e con il Piano di gestione degli incidenti di sicurezza informatica, dei quali costituisce parte complementare per i profili di prevenzione, riduzione del rischio e raccordo con i processi di gestione e trattamento delle anomalie e degli incidenti.
Il presente Piano è predisposto dal Settore A1911A - Sistema informativo regionale, con il coordinamento del Referente per la cybersicurezza e con il supporto del gruppo di lavoro interdirezionale; è sottoposto al Comitato di coordinamento direttori ai fini del raccordo interdirezionale e dell'acquisizione del relativo parere, ferma restando l'approvazione da parte degli organi o delle figure competenti secondo il d.lgs. 138/2024, l'assetto organizzativo dell'Ente e le eventuali deleghe formalmente adottate.

1.1 CONTESTO STRATEGICO

La cybersicurezza costituisce un presupposto essenziale per la continuità operativa, l'affidabilità dei servizi pubblici digitali e la tutela delle informazioni trattate dalla Regione Piemonte. La disciplina europea e nazionale di riferimento richiede ai soggetti rientranti nel relativo ambito di applicazione l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete, nonché la supervisione di tali misure da parte degli organi di amministrazione e direttivi. Tra gli elementi espressamente ricompresi dal decreto legislativo n. 138/2024 rientrano anche la gestione e la divulgazione delle vulnerabilità, nell'ambito delle misure di gestione del rischio per la sicurezza informatica.
Il presente Piano costituisce pertanto uno degli strumenti attraverso cui l'Ente assicura un presidio strutturato e proporzionato del rischio derivante da vulnerabilità di sicurezza informatica.

1.2 OBIETTIVO

Il presente Piano ha l'obiettivo di definire un quadro unitario e coerente per la gestione delle vulnerabilità di sicurezza informatica della Regione Piemonte, assicurando:

- l'identificazione tempestiva delle vulnerabilità che possono incidere su sistemi, applicazioni, infrastrutture, componenti e servizi digitali regionali;
- la valutazione delle vulnerabilità secondo criteri omogenei e proporzionati al rischio;
- la definizione e il coordinamento delle misure di trattamento, mitigazione o contenimento ritenute necessarie;
- il raccordo tra strutture regionali, referenti, soggetti tecnici e fornitori coinvolti;
- la tracciabilità delle attività svolte e delle decisioni assunte;
- la coerenza con gli obblighi normativi, con il modello organizzativo regionale e con il processo di gestione degli incidenti di sicurezza informatica.

1.3 CAMPO DI APPLICAZIONE

Il presente Piano si applica alla Regione Piemonte e alle sue strutture, con riferimento ai sistemi informativi e di rete, alle applicazioni, alle infrastrutture tecnologiche, ai servizi digitali e alle ulteriori componenti ICT che questa utilizza nello svolgimento delle proprie attività istituzionali o nell'erogazione dei propri servizi.
Il Piano si applica, per quanto di competenza:

- a tutte le Direzioni e ai Settori della Regione Piemonte;
- al personale dipendente e, nei limiti del ruolo svolto, ai collaboratori, consulenti e altri soggetti che operano su sistemi, dati, informazioni o servizi ICT regionali;
- ai fornitori e ai soggetti terzi che, in forza di rapporti contrattuali o convenzionali, realizzano, gestiscono, presidiano o manutengono sistemi, servizi, applicazioni, infrastrutture o componenti rilevanti per la Regione Piemonte;
- ai servizi e alle componenti esternalizzate o comunque affidate a soggetti terzi, per i profili di competenza dell'Ente in materia di indirizzo, controllo, monitoraggio, gestione del rischio e verifica del rispetto degli obblighi contrattuali e di sicurezza.

Rientrano nel perimetro del Piano le vulnerabilità di natura tecnica, configurativa, applicativa, infrastrutturale o di componente che possano compromettere, direttamente o indirettamente, la riservatezza, l'integrità, la disponibilità, l'autenticità o la resilienza dei sistemi informativi e di rete della Regione Piemonte o dei servizi da essa erogati.
Il Piano si applica congiuntamente agli altri documenti adottati dalla Regione Piemonte in materia di sicurezza informatica, gestione degli incidenti, continuità operativa, gestione del rischio, protezione dei dati personali e governo dei servizi e dei fornitori ICT, per quanto compatibili e pertinenti.
Il presente Piano è riesaminato periodicamente e, se necessario, aggiornato in caso di modifiche normative, organizzative o tecnologiche rilevanti, nonché in presenza di evidenze emerse nell'ambito delle attività di monitoraggio, audit, gestione degli incidenti, gestione del rischio o attuazione delle misure di sicurezza.

2 RIFERIMENTI

2.1 NORMATIVA VIGENTE

Per il quadro normativo e istituzionale generale applicabile alla sicurezza informatica della Regione Piemonte si rinvia al documento **REGP_POL01 – Organizzazione per la sicurezza informatica**, nella versione vigente.
Ai fini del presente Piano assumono particolare rilievo le disposizioni e gli atti applicabili in materia di gestione del rischio per la sicurezza informatica, gestione e divulgazione delle vulnerabilità, obblighi di raccordo con l'Agenzia per la cybersicurezza nazionale e gestione degli interventi richiesti o segnalati dalle autorità competenti.

2.2 RIFERIMENTI TECNICI

Per i riferimenti tecnici generali adottati nell'ambito dell'impianto documentale di sicurezza informatica si rinvia al documento **REGP_POL01 – Organizzazione per la sicurezza informatica**.
Ai fini del presente Piano sono inoltre utilizzati, ove pertinenti, i riferimenti tecnici specifici relativi alla gestione delle vulnerabilità, inclusi gli identificativi CVE, i criteri di severità quali CVSS, i bollettini e gli avvisi di sicurezza emessi da ACN, CSIRT Italia, produttori, fornitori e ulteriori fonti qualificate monitorate dall'Ente.

2.3 RIFERIMENTI DOCUMENTALI

I principali riferimenti interni al presente Piano sono i seguenti.

Codice documento	Titolo	Descrizione sintetica
REGP_POL01	Organizzazione per la sicurezza informatica	Definisce l'assetto organizzativo, i ruoli, le responsabilità e i raccordi per il governo della sicurezza informatica della Regione Piemonte.
REGP_PIA01	Piano di gestione degli incidenti di sicurezza informatica	Definisce il quadro generale di riferimento per la gestione degli incidenti di sicurezza informatica ed è coordinato con il presente Piano.
REGP_PIA07	Piano di continuità operativa	Definisce le misure organizzative e operative per la continuità dei

Codice documento	Titolo	Descrizione sintetica
		servizi critici e rileva per i casi in cui le vulnerabilità possano incidere sulla disponibilità dei servizi.
REGP_PR01	Procedure per la sicurezza informatica	Disciplina le modalità operative di attuazione del processo di gestione delle vulnerabilità, incluse la presa in carico delle segnalazioni, l'attivazione dei soggetti tecnici competenti, la pianificazione delle verifiche tecniche, la gestione degli esiti e delle evidenze e il monitoraggio delle azioni di trattamento.

3 GLOSSARIO

3.1 GLOSSARIO DEI TERMINI

Termine	Definizione sintetica
Vulnerabilità	Debolezza o falla di un sistema informatico, di un'applicazione, di una configurazione, di un componente o di un processo che può essere sfruttata per compromettere la riservatezza, l'integrità o la disponibilità di dati, sistemi o servizi della Regione Piemonte.
CVE - Common Vulnerabilities and Exposures	Sistema standardizzato di identificazione delle vulnerabilità di sicurezza note, basato su identificativi univoci.
CVSS - Common Vulnerability Scoring System	Sistema di valutazione della gravità delle vulnerabilità che consente di esprimere un punteggio standardizzato di severità, da utilizzare come elemento di supporto alla prioritizzazione.
Zero-day	Vulnerabilità per la quale non è ancora disponibile una correzione o una misura di trattamento ordinaria resa disponibile dal produttore, oppure la cui conoscenza pubblica e il relativo sfruttamento precedono la disponibilità della correzione.
Remediation	Insieme delle attività finalizzate alla rimozione o correzione della vulnerabilità, ad esempio tramite patch, aggiornamenti, riconfigurazioni o modifiche tecniche.
Mitigazione	Insieme delle misure tecniche o organizzative adottate per ridurre il rischio associato a una vulnerabilità quando la correzione definitiva non è immediatamente praticabile.
Vulnerability Assessment (VA)	Attività di individuazione, analisi e classificazione delle vulnerabilità presenti in sistemi, applicazioni, infrastrutture o componenti, svolta mediante verifiche tecniche automatizzate e, ove necessario, approfondimenti specialistici.
Penetration Test (PT)	Attività di verifica tecnica della sicurezza volta a simulare tentativi controllati di sfruttamento di vulnerabilità, al fine di valutare l'effettiva esposizione del sistema e l'efficacia delle misure di protezione adottate.
Coordinated Vulnerability Disclosure (CVD)	Processo strutturato di gestione delle segnalazioni esterne di vulnerabilità, finalizzato a consentire la verifica tecnica, il coordinamento con i soggetti interessati e l'eventuale trattamento della vulnerabilità prima di una sua diffusione pubblica.
Risk Acceptance	Decisione formale e tracciata di accettazione del rischio residuo associato a una vulnerabilità, adottata nei casi in cui il trattamento non sia attuabile, non sia proporzionato o richieda tempi non compatibili con l'immediata correzione.
Segnalazione di vulnerabilità	Comunicazione interna o esterna con cui viene portata all'attenzione della Regione Piemonte una vulnerabilità potenziale o accertata che interessa sistemi, applicazioni, infrastrutture, componenti o servizi di competenza dell'Ente.
Registro delle vulnerabilità	Strumento di tracciatura delle vulnerabilità identificate, delle valutazioni effettuate, delle misure di trattamento definite, dei soggetti responsabili e dello stato di avanzamento delle azioni previste.
Referente per la cybersicurezza	Figura individuata dalla Regione Piemonte per il coordinamento dell'attuazione della normativa in materia di cybersicurezza e per il presidio dei principali flussi informativi e organizzativi connessi.
ACN - Agenzia per la Cybersicurezza Nazionale	Autorità nazionale competente in materia di cybersicurezza, cui competono, secondo la normativa vigente, funzioni di regolazione, indirizzo, vigilanza e supporto.
CSIRT Italia	Struttura nazionale per la risposta agli incidenti di sicurezza informatica, operante nell'ambito dell'Agenzia per la Cybersicurezza Nazionale.
Piano di continuità operativa	Documento che definisce le misure organizzative e operative per assicurare la continuità dei servizi in caso di eventi che possano comprometterne l'erogazione.

3.2 ACRONIMI

Acronimo	Descrizione
ACN	Agenzia per la Cybersicurezza Nazionale
CAD	Codice dell'amministrazione digitale
CSIRT Italia	Computer Security Incident Response Team Italia
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
D.Lgs.	Decreto legislativo
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technology
NIS2	Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione
PCO	Piano di continuità operativa
PT	Penetration Test
RACI	Matrice delle responsabilità: Responsible, Accountable, Consulted, Informed
VA	Vulnerability Assessment
VA/PT	Vulnerability Assessment / Penetration Test

4 PRINCIPI

La gestione delle vulnerabilità dell'Ente si fonda sui principi di prevenzione, tempestività, responsabilità, proporzionalità, integrazione nei processi e miglioramento continuo, in coerenza con il quadro NIS e con le specifiche ACN applicabili.
Il presente Piano presidia in via principale, nell'ambito delle specifiche di base NIS applicabili, la misura ID.RA-08 e concorre all'attuazione della misura ID.RA-01 per i profili relativi all'identificazione, alla conferma e alla registrazione delle vulnerabilità. Il Piano si raccorda con le misure ID.RA-05 e ID.RA-06, attuate nell'ambito dei processi di valutazione e trattamento del rischio disciplinati rispettivamente dal REGP_PIA03 – Valutazione del rischio cyber e dal REGP_PIA04 – Piano di trattamento dei rischi per la sicurezza informatica.
Il Piano si raccorda altresì con le misure GV.PO-01, GV.PO-02, GV.RR-02, ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, GV.SC-02, GV.SC-04, GV.SC-05, GV.SC-07 e PR.PS-02, per i profili relativi a politiche e riesame, ruoli e responsabilità, inventari, flussi, servizi erogati dai fornitori, supply chain, obblighi contrattuali e aggiornamenti di sicurezza.
Con riferimento agli obblighi di rafforzamento della resilienza applicabili alla Regione Piemonte ai sensi della legge 28 giugno 2024, n. 90 e dei relativi atti attuativi, il presente Piano concorre altresì al presidio delle misure relative all'identificazione e documentazione delle vulnerabilità, alla loro gestione e alla ricezione, analisi e trattamento delle informazioni provenienti da fonti interne ed esterne.

4.1 PREVENZIONE E TEMPESTIVITÀ

L'Ente assicura che le vulnerabilità siano monitorate, analizzate e trattate con tempestività, in misura proporzionata alla criticità del sistema o del servizio interessato, alla gravità tecnica, al livello di esposizione, all'eventuale disponibilità di exploit pubblici e al possibile impatto sui servizi, sui dati e sulle funzioni istituzionali.
Le segnalazioni provenienti dall'Agenzia per la cybersicurezza nazionale, dal CSIRT Italia o da ulteriori autorità competenti, nonché le vulnerabilità che presentano particolare gravità o urgenza, sono trattate con priorità, secondo le tempistiche e le modalità previste dagli atti interni e dalla normativa applicabile.

4.2 ACCOUNTABILITY E OWNERSHIP

La gestione delle vulnerabilità si fonda sulla chiara attribuzione di ruoli, responsabilità e poteri. Gli organi di amministrazione e gli organi direttivi approvano le modalità di implementazione delle misure; le strutture tecniche e organizzative dell'Ente ne assicurano la concreta attuazione secondo le rispettive competenze. Questo assetto è coerente con l'articolo 23 del d.lgs. 138/2024 e con la misura ACN GV.RR-02.

4.3 PROPORZIONALITÀ E APPROCCIO RISK-BASED

La prioritizzazione non è definita sulla sola base del punteggio CVSS o di altri indicatori tecnici standardizzati, ma mediante una valutazione contestualizzata rispetto al contesto organizzativo, tecnologico e di servizio dell'Ente.

4.4 CONFORMITÀ BY DESIGN

Le esigenze di gestione delle vulnerabilità devono essere considerate, per quanto pertinente, nelle fasi di acquisizione, sviluppo, configurazione, collaudo, rilascio, esercizio, manutenzione e dismissione dei sistemi e servizi ICT. Questo principio è coerente con l'articolo 24 del d.lgs. 138/2024 e con le misure ACN sulla supply chain e sulla definizione dei requisiti di sicurezza nelle forniture.

4.5 MIGLIORAMENTO CONTINUO

Il processo di gestione delle vulnerabilità è riesaminato e migliorato sulla base di indicatori, audit, assessment, esiti delle attività di trattamento, incidenti, segnalazioni e ulteriori evidenze rilevanti.

5 GOVERNANCE E RESPONSABILITÀ

La gestione delle vulnerabilità è attuata secondo l'assetto organizzativo definito nel REGP_POL01 – Organizzazione per la sicurezza informatica. Il presente capitolo disciplina esclusivamente i raccordi e le responsabilità specifiche necessarie all'attuazione del processo di gestione delle vulnerabilità.

5.1 MODELLO ORGANIZZATIVO

In merito ai ruoli si rimanda al documento REGP_POL01.

5.2 RUOLI E RESPONSABILITÀ (TABELLA RACI)

Legenda:

- **R** = Responsible, soggetto che esegue o concorre operativamente all'attività;
- **A** = Accountable, soggetto responsabile del presidio complessivo o dell'esito dell'attività;
- **C** = Consulted, soggetto consultato;
- **I** = Informed, soggetto informato.

Processo / attività		Settore A1911A	Referente per la cybersicurezza	Punto di contatto NIS2	Referente CSIRT	SOC	Fornitori / soggetti terzi / eventuale in house
Monitoraggio delle fonti, presa in carico e prima qualificazione delle vulnerabilità		R	A	C	C	R	C
Aggiornamento delle informazioni utili alla correlazione tra vulnerabilità, asset, servizi, prodotti e		A	C	I	I	C	R

componenti							
Verifica di applicabilità e impatto sui sistemi, servizi o componenti regionali		R	A	I		C	R
Classificazione, prioritizzazione e definizione delle misure di trattamento		R	A	I	I	C	C
Attivazione di fornitori, soggetti terzi o soggetti in house e richiesta di piani di intervento o evidenze		A/R	C	I	I	C	R
Monitoraggio delle azioni di trattamento e verifica delle evidenze di esito		A/R	C	I	I	R	R
Raccordo con il processo di gestione degli incidenti, ove necessario		C	A	C	R	C	C
Interlocuzioni con ACN per profili NIS o richieste istituzionali relative a vulnerabilità		C	C	A/R	C	C	I
Interlocuzioni operative con CSIRT Italia, ove previste		C	C	A	R	C	I
Individuazione delle azioni di miglioramento del processo		R	C	I	I	C	C

5.3 DESCRIZIONE DEI RUOLI

Per il dettaglio dei ruoli e delle responsabilità generali si rinvia al documento **REGP_POL01 – Organizzazione per la sicurezza informatica**. Le descrizioni che seguono sono limitate alle attività rilevanti per il processo di gestione delle vulnerabilità.

Settore A1911A - Sistema informativo regionale

Cura il coordinamento tecnico-organizzativo del processo di gestione delle vulnerabilità, il raccordo con le strutture coinvolte e il monitoraggio dello stato di avanzamento delle azioni di trattamento.

Referente per la cybersicurezza

Presidia complessivamente il processo, ne assicura la coerenza con il modello di sicurezza informatica regionale e coordina reporting, riesame ed eventuali escalation.

Punto di contatto NIS2

Assicura, per quanto di competenza, il raccordo con gli adempimenti e i flussi istituzionali NIS, nei casi in cui la gestione della vulnerabilità richieda interlocuzioni o riscontri verso ACN.

Referente CSIRT

Cura, per quanto di competenza, le interlocuzioni operative con CSIRT Italia, incluse quelle connesse a segnalazioni, notifiche o raccordi con il processo di gestione degli incidenti.

SOC

Supporta il monitoraggio delle fonti, la prima analisi tecnica, la classificazione delle vulnerabilità e il controllo dell'avanzamento delle azioni di trattamento.

Per la Regione Piemonte il servizio SOC è assicurato da CSI Piemonte nei limiti dei rapporti di servizio vigenti. Tale supporto non modifica l'attribuzione delle responsabilità organizzative, decisionali e di controllo in capo alla Regione Piemonte.

Fornitori

Eseguono, per quanto previsto dai rapporti contrattuali o convenzionali, le verifiche tecniche, gli aggiornamenti, le mitigazioni e gli ulteriori interventi richiesti, fornendo le relative evidenze.

6 REQUISITI DI CONFORMITÀ E OBBLIGHI NORMATIVI

La gestione delle vulnerabilità costituisce parte integrante delle misure di gestione del rischio per la sicurezza informatica dell'Ente. Il d.lgs. 138/2024 prevede che i soggetti NIS adottino misure tecniche, operative e organizzative adeguate e proporzionate e include espressamente, tra tali misure, la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità. Le specifiche di base ACN vigenti, adottate nell'ambito della disciplina NIS, costituiscono il riferimento attuativo di base per gli obblighi degli articoli 23, 24, 25, 29 e 32 del decreto NIS.

Il presente Piano definisce il quadro generale di riferimento con cui l'Ente assicura la conformità ai requisiti normativi e regolatori applicabili in materia di gestione delle vulnerabilità, in raccordo con il documento di Organizzazione della sicurezza informatica, con la procedura operativa di gestione delle vulnerabilità e con il piano di gestione degli incidenti di sicurezza informatica.

6.1 OBBLIGHI NORMATIVI

La gestione delle vulnerabilità è attuata in coerenza con il quadro normativo e regolatorio richiamato nel capitolo 2, con particolare riferimento al d.lgs. 4 settembre 2024, n. 138 e alle specifiche di base ACN applicabili alla Regione Piemonte.

Le modalità di attuazione sono definite dal presente Piano, dalla procedura operativa di gestione delle vulnerabilità e dagli ulteriori documenti dell'impianto di sicurezza informatica regionale.

Gli avvisi, le segnalazioni o le richieste di ACN, CSIRT Italia o altre autorità competenti relativi a specifiche vulnerabilità sono presi in carico con priorità, secondo le modalità previste dagli atti applicabili.

Con riferimento alle specifiche vulnerabilità puntualmente segnalate dall'Agenzia per la cybersicurezza nazionale nell'ambito degli obblighi applicabili alla Regione Piemonte ai sensi della legge 28 giugno 2024, n. 90, l'Ente adotta gli interventi indicati dall'Agenzia senza ritardo e comunque non oltre quindici giorni dalla segnalazione. Qualora motivate esigenze di natura tecnico-organizzativa impediscano l'adozione degli interventi o ne comportino il differimento oltre il termine previsto, è assicurata tempestiva comunicazione all'Agenzia secondo le modalità applicabili. La presa in carico, le azioni attuate e gli eventuali differimenti sono tracciati secondo le procedure dell'Ente.

6.2 CLASSIFICAZIONE E CRITERI DI GESTIONE DELLE TEMPISTICHE

Le vulnerabilità identificate sono classificate secondo criteri omogenei, tenendo conto almeno della gravità tecnica, della criticità del sistema o del servizio interessato, del livello di esposizione, della possibile sfruttabilità, della presenza di misure compensative e del potenziale impatto sui servizi, sui dati e sulle funzioni istituzionali della Regione Piemonte.

Le tempistiche di riferimento, le soglie di escalation, i criteri di priorità e le eventuali condizioni di deroga sono definiti nella procedura operativa di riferimento. Eventuali scostamenti rispetto alle tempistiche

ordinarie devono essere motivati e tracciati; ove comportino un differimento del trattamento o l'accettazione di un rischio residuo, sono gestiti secondo la metodologia di valutazione del rischio e il Piano di trattamento dei rischi adottati dall'Ente.

6.3 PRESIDI DI SICUREZZA NEL CICLO DI VITA DEI SISTEMI, DEI SERVIZI ICT E DEI RAPPORTI CON I FORNITORI

La gestione delle vulnerabilità è considerata dalla Regione Piemonte nell'ambito delle attività di acquisizione, affidamento, configurazione, modifica, manutenzione, evoluzione e dismissione dei sistemi informativi e di rete, delle applicazioni e dei servizi ICT utilizzati per lo svolgimento delle attività istituzionali e per l'erogazione dei servizi regionali.
La Regione assicura, secondo criteri di proporzionalità e in coerenza con le responsabilità contrattuali e organizzative applicabili, un presidio di governo e controllo volto a considerare i requisiti di sicurezza e di gestione delle vulnerabilità nelle fasi rilevanti del ciclo di vita dei sistemi e dei servizi ICT.
A tal fine, per quanto pertinente rispetto alla tipologia di servizio, al livello di criticità del sistema o servizio interessato, al modello di affidamento e agli obblighi contrattuali applicabili, la Regione Piemonte promuove e verifica:

- l'inserimento di requisiti di sicurezza e di gestione delle vulnerabilità negli atti di acquisizione, affidamento, convenzione o contratto relativi a sistemi, applicazioni, infrastrutture, servizi cloud, servizi SaaS o altri servizi ICT;
- la previsione, nei rapporti con fornitori e soggetti terzi, di obblighi informativi relativi a vulnerabilità note, aggiornamenti di sicurezza, patch, misure di mitigazione, configurazioni sicure e incidenti o eventi rilevanti che possano incidere sui servizi regionali;
- l'acquisizione di evidenze adeguate circa la gestione delle vulnerabilità da parte dei fornitori, ivi incluse, ove applicabile, attestazioni, report, esiti di verifiche tecniche, piani di remediation, comunicazioni di sicurezza del produttore o del fornitore e riscontri sulle azioni correttive adottate;
- la valutazione dell'opportunità di richiedere verifiche tecniche di sicurezza, vulnerability assessment, penetration test o ulteriori controlli prima della messa in esercizio di nuovi sistemi o in occasione di modifiche significative, in funzione della criticità del servizio, dell'esposizione, dei dati trattati e del rischio associato;
- il raccordo tra gestione delle vulnerabilità, gestione delle modifiche, patch management, gestione degli asset, gestione dei fornitori e gestione degli incidenti di sicurezza informatica;
- la tracciabilità delle decisioni assunte nei casi in cui una vulnerabilità non possa essere risolta nei tempi ordinariamente previsti o richieda misure temporanee di mitigazione, accettazione del rischio residuo o escalation verso i livelli decisionali competenti.

Per i servizi, le applicazioni o le infrastrutture integralmente gestiti da fornitori, soggetti terzi o soggetti in house, la Regione Piemonte esercita il proprio presidio mediante attività di indirizzo, richiesta e valutazione delle evidenze, verifica del rispetto degli obblighi contrattuali e raccordo con le strutture competenti, senza sostituirsi alle responsabilità operative e tecniche attribuite ai soggetti incaricati della realizzazione, gestione o manutenzione del servizio.
Le modalità operative di dettaglio, le eventuali soglie di criticità, le evidenze richieste, i flussi di interlocuzione con i fornitori e i criteri per l'attivazione di verifiche tecniche sono disciplinati nella procedura di gestione delle vulnerabilità, negli atti contrattuali applicabili e negli ulteriori documenti organizzativi o procedurali adottati dalla Regione Piemonte.

7 PROCESSI

La Regione Piemonte attua il processo di gestione delle vulnerabilità mediante attività coordinate di monitoraggio delle fonti informative, presa in carico e verifica di applicabilità delle vulnerabilità, attivazione dei soggetti tecnici e contrattuali competenti, acquisizione delle evidenze disponibili e monitoraggio delle

azioni di trattamento, in coerenza con il presente Piano, con la procedura operativa di riferimento e con il modello organizzativo della sicurezza informatica.

7.1 GESTIONE DELLE FONTI INFORMATIVE E DELLE INFORMAZIONI SUI SISTEMI E COMPONENTI MONITORATI

La Regione Piemonte assicura il monitoraggio strutturato delle fonti informative istituzionali, tecniche e dei fornitori rilevanti ai fini dell'individuazione delle vulnerabilità che possano interessare sistemi, applicazioni, infrastrutture, componenti e servizi di propria competenza.

Le fonti informative comprendono, almeno per quanto pertinenti:

- i canali istituzionali dell'Agenzia per la cybersicurezza nazionale e del CSIRT Italia;
- i bollettini e gli avvisi dei produttori e dei fornitori delle tecnologie in uso;
- le ulteriori fonti tecniche utilizzate nell'ambito del presidio di sicurezza, ivi incluse le basi informative standardizzate di settore;
- gli esiti di verifiche tecniche, assessment, incidenti, change rilevanti e segnalazioni interne o esterne.

Il monitoraggio delle fonti informative è svolto con il supporto del SOC, che assicura la raccolta e la prima analisi tecnica delle informazioni rilevanti; il Settore A1911A - Sistema informativo regionale coordina il processo e assicura il raccordo con le strutture competenti per materia, con i fornitori e con gli altri soggetti coinvolti.

La Regione Piemonte mantiene, secondo le modalità organizzative e strumentali adottate, un insieme strutturato di informazioni sui sistemi, sui servizi, sui prodotti e sui componenti software oggetto di monitoraggio, funzionale alla verifica dell'applicabilità delle vulnerabilità e alla definizione delle priorità di intervento.

Le modalità operative di gestione delle fonti informative, di aggiornamento delle informazioni utili all'identificazione dei sistemi monitorati e di tracciatura delle attività sono definite nella procedura operativa di riferimento.

7.2 PRESA IN CARICO, VERIFICA DI APPLICABILITÀ E TRATTAMENTO DELLE VULNERABILITÀ

La Regione Piemonte assicura la presa in carico delle vulnerabilità potenzialmente rilevanti per i propri sistemi informativi e di rete mediante un processo organizzativo fondato sul monitoraggio delle fonti informative, sulla verifica della possibile applicabilità al contesto regionale, sull'attivazione dei soggetti tecnici e contrattuali competenti e sulla tracciabilità delle decisioni e degli esiti.
L'individuazione delle vulnerabilità potenzialmente rilevanti avviene, in via ordinaria, attraverso l'analisi delle informazioni provenienti da fonti istituzionali, tecniche e contrattuali, ivi inclusi gli avvisi dell'Agenzia per la cybersicurezza nazionale e del CSIRT Italia, i bollettini dei produttori e dei fornitori delle tecnologie in uso, le comunicazioni dei soggetti che gestiscono o presidiano servizi e componenti ICT regionali, gli esiti di incidenti, assessment, change rilevanti e ulteriori segnalazioni interne o esterne.
La Regione Piemonte mantiene, secondo le modalità organizzative e strumentali adottate, le informazioni necessarie a correlare le vulnerabilità note con i sistemi, i servizi, le applicazioni, le infrastrutture, le componenti tecnologiche e i servizi ICT di propria competenza o comunque utilizzati nell'esercizio delle

funzioni istituzionali. Tali informazioni sono utilizzate per supportare la verifica della possibile applicabilità delle vulnerabilità e per individuare i soggetti competenti alla relativa presa in carico.
Nell'ambito delle iniziative finalizzate al rafforzamento della sicurezza del software realizzato per conto dell'Ente, la Regione Piemonte ha commissionato e adottato la piattaforma **CODEMETRIC**, sviluppata nell'ambito della progettualità "Avviso 3", quale strumento di supporto alla valutazione della qualità del codice e all'individuazione delle vulnerabilità dei prodotti software sottoposti ad analisi.
Gli esiti prodotti dalla piattaforma concorrono, unitamente alle ulteriori fonti informative e verifiche previste dal presente Piano, alla qualificazione delle vulnerabilità, alla valutazione della loro rilevanza e alla definizione delle eventuali azioni di trattamento.
La Regione Piemonte promuove la progressiva estensione dell'utilizzo di CODEMETRIC ai prodotti software realizzati, evoluti o manutenuti per conto dell'Ente, secondo criteri di priorità, proporzionalità, sostenibilità tecnica e coerenza con le modalità di affidamento e gestione dei servizi ICT.

Quando una vulnerabilità risulta potenzialmente applicabile a sistemi, servizi, prodotti o componenti utilizzati dalla Regione Piemonte, il Settore A1911A - Sistema informativo regionale, con il supporto del Referente per la cybersicurezza e del SOC, assicura il raccordo con le strutture competenti per materia, con i fornitori, con i soggetti terzi e con gli eventuali soggetti in house coinvolti nella realizzazione, gestione, manutenzione o presidio dei sistemi interessati.
La verifica di applicabilità e di impatto è svolta sulla base delle informazioni disponibili e, ove necessario, mediante richiesta di riscontro ai fornitori o ai soggetti tecnici competenti. Tale verifica è finalizzata almeno a:

- identificare il riferimento tecnico della vulnerabilità, ove disponibile;
- individuare i sistemi, i servizi, le applicazioni, le infrastrutture o le componenti potenzialmente interessate;
- acquisire conferma circa l'effettiva esposizione o non esposizione del sistema o servizio alla vulnerabilità;
- valutare la gravità tecnica, il livello di esposizione e il potenziale impatto sui servizi, sui dati e sulle funzioni istituzionali;
- individuare le misure di correzione, mitigazione, contenimento o monitoraggio applicabili;
- definire i soggetti responsabili dell'attuazione delle azioni richieste e dei relativi riscontri.

Per i sistemi, servizi o componenti gestiti da fornitori, soggetti terzi o soggetti in house, la Regione Piemonte non si sostituisce alle responsabilità operative e tecniche attribuite ai soggetti incaricati della gestione o manutenzione del servizio, ma assicura il presidio di propria competenza attraverso la richiesta di riscontri, evidenze, piani di intervento, conferme di non applicabilità, attestazioni di avvenuta correzione o indicazioni sulle misure temporanee di mitigazione adottate.
Le vulnerabilità che presentano maggiore gravità tecnica, elevato livello di esposizione, disponibilità di exploit pubblici, possibile impatto significativo sui servizi regionali o rilievo istituzionale sono trattate con priorità. Le segnalazioni provenienti dall'Agenzia per la cybersicurezza nazionale, dal CSIRT Italia o da ulteriori autorità competenti sono prese in carico senza indebito ritardo, secondo le modalità definite nella procedura operativa di riferimento e negli atti applicabili.
Le attività di Vulnerability Assessment, Penetration Test e le ulteriori verifiche tecniche di sicurezza sono pianificate dalla Regione Piemonte nell'ambito del programma di gestione delle vulnerabilità, secondo criteri di priorità e proporzionalità.
La pianificazione tiene conto, in particolare, della criticità dei sistemi e dei servizi, del livello di esposizione, della natura dei dati trattati, degli obblighi normativi e contrattuali, del modello di gestione del servizio, degli esiti dell'analisi del rischio e della disponibilità dei soggetti tecnici competenti.

Per i sistemi informativi e di rete ritenuti rilevanti, la Regione Piemonte inserisce nel programma periodico di verifica tecnica attività di identificazione delle vulnerabilità, anche mediante Vulnerability Assessment, Penetration Test, analisi specialistiche, verifiche svolte dai fornitori o da altri soggetti qualificati.
Nei casi in cui le verifiche non siano svolte direttamente dalla Regione Piemonte, l'Ente richiede ai soggetti responsabili della gestione tecnica del servizio la produzione di report, attestazioni o ulteriori evidenze documentali idonee a dimostrare l'esecuzione delle attività, gli esiti rilevati e le eventuali azioni di trattamento previste.
La periodicità, l'estensione e le modalità delle verifiche sono definite nel relativo programma, riesaminate in funzione dell'evoluzione del rischio e aggiornate in presenza di modifiche significative dei sistemi, dei servizi o del contesto di minaccia.
Per i nuovi sistemi o servizi e in occasione di modifiche rilevanti, la Regione Piemonte valuta, secondo criteri di proporzionalità e sulla base del modello di acquisizione o gestione adottato, la necessità di acquisire evidenze di sicurezza, richiedere verifiche tecniche, ottenere conferme dai fornitori o prevedere condizioni di rilascio connesse alla gestione delle vulnerabilità note e alla disponibilità delle misure di correzione o mitigazione.
Il presidio continuativo delle vulnerabilità è assicurato mediante un insieme coordinato di attività che comprende il monitoraggio delle fonti informative, le verifiche tecniche pianificate secondo rischio e criticità, il raccordo con fornitori e soggetti tecnici competenti, la gestione delle segnalazioni, la tracciatura delle vulnerabilità rilevanti, l'acquisizione degli esiti delle verifiche disponibili e il monitoraggio dell'attuazione delle azioni di correzione o mitigazione.
Gli esiti delle attività di presa in carico, verifica di applicabilità, classificazione, richiesta di intervento, monitoraggio e chiusura sono tracciati negli strumenti adottati dalla Regione Piemonte per la gestione delle vulnerabilità. Le modalità operative di dettaglio, incluse le tempistiche, i flussi di interlocuzione con i fornitori, le evidenze richieste, le condizioni di escalation, i criteri di accettazione del rischio residuo e le modalità di chiusura, sono definite nella procedura operativa di riferimento.

7.3 GESTIONE DELLE SEGNALAZIONI ESTERNE DI VULNERABILITÀ

La Regione Piemonte assicura la gestione tracciata delle eventuali segnalazioni esterne di vulnerabilità che riguardino sistemi, servizi o componenti di propria competenza, secondo modalità coerenti con il presente Piano e con gli atti organizzativi e procedurali adottati.
Le segnalazioni pervenute attraverso canali istituzionali o, ove previsti, attraverso specifici canali dedicati, sono sottoposte a verifica tecnica preliminare con il supporto del SOC e con il coinvolgimento delle strutture competenti per materia e dei fornitori eventualmente interessati.
Qualora la segnalazione risulti fondata o meritevole di approfondimento, essa è presa in carico nell'ambito del processo di gestione delle vulnerabilità, con definizione delle misure di analisi, mitigazione o correzione ritenute necessarie.
La gestione delle segnalazioni esterne avviene nel rispetto dei principi di riservatezza, tracciabilità, proporzionalità e coordinamento con i soggetti interessati. Qualora la vulnerabilità segnalata presenti profili tali da richiedere ulteriori valutazioni istituzionali o procedurali, la Regione Piemonte assicura il raccordo con i soggetti competenti secondo le modalità previste dagli atti applicabili.
Le modalità di ricezione, presa in carico, verifica, eventuale interlocuzione con il segnalante e gestione degli esiti sono definite nella procedura operativa di riferimento.
Qualora la Regione Piemonte adotti specifiche modalità di Coordinated Vulnerability Disclosure, i relativi canali, criteri e modalità operative sono disciplinati nei presidi procedurali o tecnici individuati dall'Ente.

8 REPORTING, RIESAME ED ESCALATION

La Regione Piemonte adotta un sistema di reporting e riesame finalizzato ad assicurare una visione periodica sul livello di esposizione alle vulnerabilità, sullo stato di attuazione delle misure di trattamento, sulle criticità rilevanti e sull'efficacia complessiva del presente Piano.
Il reporting e il riesame sono coordinati dal Referente per la cybersicurezza, con il supporto del Settore A1911A - Sistema informativo regionale, del SOC e delle strutture competenti per materia, secondo le rispettive competenze.

8.1 REPORTING PERIODICO E RIESAME DIREZIONALE

Il Referente per la cybersicurezza predispone, con cadenza almeno annuale e, ove necessario, con frequenza maggiore in relazione al livello di esposizione, alla criticità delle vulnerabilità rilevate o a specifiche esigenze organizzative, un rapporto riepilogativo sulla gestione delle vulnerabilità da sottoporre al Comitato di coordinamento direttori quale sede di raccordo direzionale e interdirezionale.
Il rapporto contiene:

- il quadro sintetico delle vulnerabilità rilevate, classificate e prese in carico nel periodo di riferimento;
- lo stato di avanzamento delle azioni di correzione, mitigazione, contenimento o monitoraggio;
- le vulnerabilità critiche o di maggiore impatto ancora aperte;
- gli eventuali ritardi, scostamenti o criticità rilevanti rispetto alle tempistiche o alle priorità definite;
- gli esiti delle verifiche tecniche, degli assessment, delle attività di controllo o delle evidenze acquisite da fornitori, soggetti terzi o soggetti in house, ove disponibili;
- le criticità ricorrenti o sistemiche emerse nella gestione delle vulnerabilità;
- il livello complessivo di esposizione residua rispetto ai sistemi, servizi o componenti maggiormente rilevanti;
- gli eventuali rischi residui che richiedano valutazione, accettazione formale o escalation verso i livelli decisionali competenti;
- le esigenze di aggiornamento del presente Piano, della procedura operativa, degli strumenti di tracciatura o delle ulteriori misure organizzative, tecniche o contrattuali.

Il Comitato di coordinamento direttori esamina il rapporto per i profili di propria competenza, valuta gli elementi di attenzione di rilievo trasversale e favorisce il raccordo tra le Direzioni e le strutture regionali interessate. Le eventuali decisioni, azioni organizzative, misure di trattamento o atti conseguenti sono assunti dai soggetti competenti secondo l'assetto organizzativo e le responsabilità vigenti.
Gli esiti del riesame sono tracciati secondo le modalità organizzative adottate dall'Ente e costituiscono base per l'aggiornamento del presente Piano, della procedura operativa e delle ulteriori misure ritenute necessarie.

8.2 COMUNICAZIONI STRAORDINARIE ED ESCALATION

Oltre al reporting periodico, il Referente per la cybersicurezza assicura comunicazioni straordinarie nei casi in cui emergano situazioni che richiedano valutazioni, decisioni o indirizzi tempestivi da parte delle strutture competenti o del Comitato di coordinamento direttori.
Rientrano, in particolare, tra le situazioni che possono richiedere escalation:

- la presenza di vulnerabilità critiche che interessino sistemi o servizi rilevanti e che non possano essere trattate nei tempi ordinari;
- la presenza di vulnerabilità per le quali si rilevi un rischio elevato di sfruttamento o un potenziale impatto significativo sui servizi regionali;

- il mancato riscontro, da parte di fornitori, soggetti terzi o soggetti in house, rispetto a richieste di verifica, trattamento o evidenza relative a vulnerabilità rilevanti;
- la necessità di accettare formalmente un rischio residuo connesso alla mancata o differita risoluzione di una vulnerabilità;
- il verificarsi di situazioni in cui una vulnerabilità nota abbia determinato o possa determinare un incidente di sicurezza informatica;
- la ricezione di avvisi, segnalazioni o richieste da parte di soggetti istituzionali competenti che richiedano una presa in carico urgente;
- l'emersione di criticità sistemiche o di elementi che rendano necessario rivedere priorità, misure, responsabilità, risorse o modalità organizzative.

Le comunicazioni straordinarie sono effettuate secondo le modalità e i canali definiti negli atti interni applicabili, assicurando tracciabilità, riservatezza e coerenza con il processo di gestione degli incidenti di sicurezza informatica, ove pertinente.

9 MIGLIORAMENTO CONTINUO

La Regione Piemonte persegue un approccio di miglioramento continuo della gestione delle vulnerabilità, finalizzato ad accrescere progressivamente l'efficacia del processo, la tempestività delle azioni di trattamento e la coerenza complessiva tra misure organizzative, tecniche e procedurali.
A tal fine, la Regione Piemonte assicura:

- l'analisi delle vulnerabilità ricorrenti, delle criticità sistemiche e delle relative cause;
- il monitoraggio degli indicatori utili a valutare l'andamento del processo e l'efficacia delle misure adottate;
- l'integrazione delle evidenze derivanti da audit, assessment, incidenti, change rilevanti e segnalazioni interne o esterne;
- l'aggiornamento periodico del presente Piano, della procedura operativa e degli eventuali strumenti di supporto adottati;
- il progressivo affinamento dei criteri di classificazione, prioritizzazione, trattamento e monitoraggio delle vulnerabilità.

Le attività di miglioramento continuo tengono conto del principio di proporzionalità e del contesto operativo della Regione Piemonte. L'adozione di strumenti o modalità più evolute di monitoraggio o verifica è valutata in funzione dell'effettiva utilità, della sostenibilità organizzativa e del livello di rischio dei sistemi e dei servizi interessati.

9.1 DIFFUSIONE E CONSAPEVOLEZZA

Il presente Piano è reso disponibile nell'ambito dei sistemi documentali interni della Regione Piemonte e nei canali interni individuati per la consultazione della documentazione organizzativa e procedurale in materia di cybersicurezza.
La diffusione del Piano è assicurata nei confronti delle strutture regionali e dei soggetti interni interessati, in relazione alle rispettive competenze e responsabilità, nonché, ove necessario, nei confronti dei soggetti esterni che concorrono alla gestione dei sistemi o dei servizi interessati, nei limiti di pertinenza e secondo le modalità organizzative e contrattuali applicabili.
La Regione Piemonte promuove iniziative di informazione e consapevolezza rivolte ai soggetti coinvolti nel processo di gestione delle vulnerabilità, con particolare riferimento ai ruoli tecnici, organizzativi e di coordinamento, al fine di assicurare la conoscenza delle responsabilità, dei flussi operativi e delle modalità di segnalazione e presa in carico previste.
Restano ferme le ordinarie forme di pubblicazione dei documenti, dei dati e delle informazioni organizzative la cui pubblicazione sia prevista dalla normativa applicabile o dagli atti organizzativi dell'Ente.

L'eventuale diffusione esterna di ulteriori contenuti del presente Piano è valutata dalla Regione Piemonte secondo criteri di pertinenza, proporzionalità e tutela delle informazioni organizzative e di sicurezza.

VERIFICHE ED APPROVAZIONI

VERSIONE	REDAZIONE		CONTROLLO APPROVAZIONE		AUTORIZZAZIONE EMISSIONE	
	NOME	DATA	NOME	DATA	NOME	DATA

STATO DELLE VARIAZIONI

VERSIONE	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
V01	Tutto il documento	Versione iniziale del documento

SOMMARIO

1 SCOPO DEL DOCUMENTO....2
2 CAMPO DI APPLICAZIONE....2
3 DEFINIZIONI....2
4 RIFERIMENTI....3
5 RUOLI E RESPONSABILITÀ....3
6 RISK MANAGEMENT: PROCESSO E METODOLOGIA....4
6.1 DEFINIZIONE DEL CONTESTO....4
6.2 VALUTAZIONE DEL RISCHIO (RISK ASSESSMENT)....5
IDENTIFICAZIONE DEI RISCHI....5
ANALISI DEI RISCHI....6
PONDERAZIONE DEI RISCHI....9
6.3 ESITI DELLE VALUTAZIONI DEL RISCHIO....10
6.4 TRATTAMENTO DEI RISCHI....11
6.4.1 Deroghe....12
6.5 MONITORAGGIO E RIESAME....12
6.6 COMUNICAZIONE E CONSULTAZIONE....13

1 SCOPO DEL DOCUMENTO

Il presente documento descrive il modello di riferimento adottato da Regione Piemonte per l'identificazione, l'analisi e la ponderazione dei rischi cyber e per la determinazione del relativo livello di rischio.
Il documento definisce la metodologia di valutazione e riporta una rappresentazione sintetica degli esiti delle valutazioni effettuate. Il dettaglio analitico delle valutazioni è mantenuto negli strumenti operativi di supporto adottati dall'Ente. Gli esiti della valutazione costituiscono uno degli elementi di ingresso del distinto processo di trattamento del rischio.
Gli scenari per i quali risultano necessarie azioni di trattamento sono gestiti mediante il REGP_PIA04 – Piano di trattamento dei rischi per la sicurezza informatica.

2 CAMPO DI APPLICAZIONE

Il modello si applica alla gestione dei rischi cyber che potrebbero compromettere la disponibilità, la riservatezza e l'integrità delle informazioni gestite attraverso i sistemi informativi e di rete di Regione Piemonte.
Sono inclusi nel campo di applicazione i rischi derivanti dalla catena di fornitura.
Le strategie adottate potranno variare in base alla natura e alla gravità dei rischi identificati, nonché alle specifiche esigenze operative e agli obiettivi dell'Ente.
L'approccio alla gestione del rischio definito deve essere recepito e rispettato da tutti i dipendenti, i dirigenti e dai membri degli Organi Direttivi.
Il processo di gestione del rischio cyber si applica al perimetro di sicurezza dell'Ente, comprensivo dei sistemi informativi e di rete, dei servizi digitali, dei dati trattati e delle dipendenze rilevanti da fornitori, soggetti in house o altre terze parti.

3 DEFINIZIONI

Pericolo / Minaccia	Proprietà o qualità intrinseca di un determinato fattore interno o esterno avente la potenzialità di causare danni.
Vulnerabilità/Punti di debolezza	Suscettibilità intrinseche all'organizzazione che hanno la potenzialità di concorrere alla concretizzazione di una minaccia.
Rischio	Evento futuro incerto capace di influenzare il raggiungimento degli obiettivi dell'organizzazione[1]. La norma ISO 31000 lo identifica come "effetto dell'incertezza sugli obiettivi". Può assumere accezione sia negativa sia positiva (opportunità).
Rischio Inerente	Evento che può verificarsi in assenza di controlli ovvero di qualsiasi azione intrapresa dal management al fine di alterarne favorevolmente la probabilità di accadimento e/o la severità delle conseguenze.
Rischio residuo o ritenuto	Parte di rischio che non è stato possibile eliminare a seguito dell'adozione delle contromisure di trattamento e che, dunque, l'ente assume di voler ritenere.
Risk Register	Elenco delle minacce identificate, da sottoporre a valutazione
Analisi del rischio	Processo di analisi del rischio attraverso tecniche di analisi qualitative, quantitative o ibride, dato dalla misurazione della probabilità di accadimento rispetto alla severità degli impatti.
Ponderazione del rischio	Confronto tra i risultati dell'analisi del rischio rispetto ai criteri definiti dal

[1] Il rischio è comunemente associato ad un evento negativo, una minaccia o una perdita. In generale, tuttavia, secondo l'accezione anglosassone (il termine risk è meno preciso e restrittivo rispetto all'italiano), il rischio può essere associato a un significato più ampio, inclusivo del concetto di opportunità; si pensi all'esempio dei rischi finanziari di tasso, interesse o cambio.

	management e dalle soglie di accettabilità.
Key Risk Indicator (KRI)	Indicatori che hanno lo scopo di misurare l'evoluzione del rischio nel tempo e che costituiscono elementi "sentinella" rispetto ai criteri definiti dall'organizzazione.
Rischio attuale	Valore del rischio al momento della valutazione, tenuto conto delle contromisure e dei presidi già attuati.
Misura di trattamento del rischio	Misura definita dal Risk Owner e validata da Sicurezza, Privacy e Continuità operativa che ha lo scopo di mitigare un rischio così da ricondurlo all'interno delle soglie di accettabilità definite dall'organizzazione. Possono consistere nell'eliminazione, nella mitigazione, nel trasferimento o nella ritenzione / accettazione.
Risk Owner (RO)	Soggetto o struttura responsabile, secondo l'assetto organizzativo dell'Ente, del servizio, processo, sistema o ambito cui il rischio si riferisce. Concorre alla valutazione del rischio, alla definizione delle azioni di trattamento e al monitoraggio dell'evoluzione del rischio, in raccordo con la struttura competente in materia di sicurezza informatica.
Referente operativo	Persona o struttura individuata dal Responsabile del rischio per fornire supporto operativo nella raccolta delle informazioni, nella valutazione dello scenario di rischio e nel monitoraggio delle azioni di trattamento.
Action Owner (AO)	Soggetto o struttura responsabile dell'attuazione di una o più azioni di trattamento individuate nel piano di trattamento dei rischi. Cura l'esecuzione delle attività assegnate e fornisce gli aggiornamenti sul relativo stato di avanzamento.
Controlli di II Livello	Sono i controlli effettuati da aree indipendenti e autonome rispetto ai Risk Owner che, per loro natura, sono preposte a coprire ambiti o tematiche del sistema di controllo interno, oppure rischi settoriali a livelli più elevati.
Controlli di III Livello	Sono i controlli effettuati dalle funzioni di garanzia interne all'organizzazione che hanno lo scopo di fornire *assurance* in relazione al processo di valutazione dei rischi.

4 RIFERIMENTI

Il presente documento fa parte dell'impianto documentale dell'Ente in materia di sicurezza informatica e deve essere letto congiuntamente al documento "REGP_POL01 – Organizzazione per la sicurezza informatica", nella versione vigente.
Al documento REGP_POL01 si rinvia per il quadro normativo e istituzionale di riferimento e per la definizione dei ruoli, delle responsabilità e dei raccordi organizzativi applicabili al processo di gestione del rischio. Gli esiti analitici delle valutazioni sono documentati negli assessment REGP_RSK01, REGP_RSK02, REGP_RSK03 e REGP_RSK04, mentre le decisioni e le azioni conseguenti al trattamento dei rischi sono disciplinate nel REGP_PIA04 – Piano di trattamento dei rischi per la sicurezza informatica.

5 RUOLI E RESPONSABILITÀ

I ruoli e le responsabilità applicabili al processo di valutazione del rischio cyber sono quelli definiti nel documento "REGP_POL01 – Organizzazione per la sicurezza informatica".
Il presente documento non introduce nuovi ruoli organizzativi né modifica le responsabilità già attribuite dall'Ente. Esso descrive le modalità con cui i soggetti e le strutture individuati nel REGP_POL01 concorrono, secondo le rispettive competenze, alle attività di valutazione, trattamento, monitoraggio e riesame del rischio cyber.
Le responsabilità operative di dettaglio sono riportate, ove necessario, negli strumenti di supporto al processo, quali registro dei rischi, piano di trattamento e relative matrici di responsabilità.

6 Risk Management: Processo e metodologia

La metodologia attuata è conforme al processo definito dallo standard **ISO 31000.** Esso definisce principi e linee guida per l'identificazione, l'analisi, la valutazione e il trattamento dei rischi, come indicato nella seguente rappresentazione grafica.

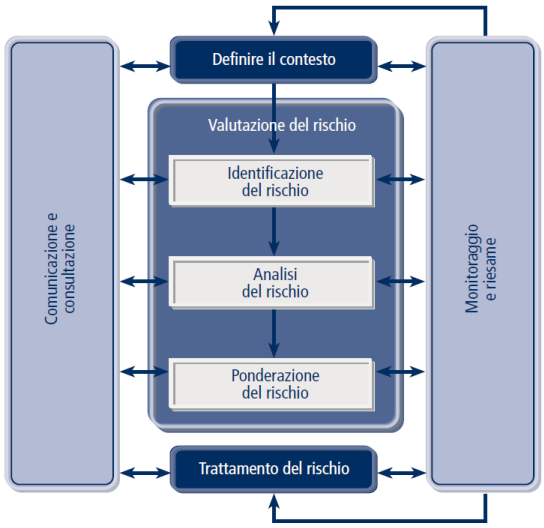


Figura 1 - Linee guida ISO 31000

Il processo di Risk Management è costituito da 5 macrofasi, di seguito elencate:

- Definizione del contesto
- Valutazione del rischio, suddivisa nelle fasi di:
  - Identificazione del rischio
  - Analisi del rischio
  - Ponderazione del rischio
- Trattamento del Rischio
- Comunicazione e Consultazione
- Monitoraggio e riesame

Le fasi di valutazione e trattamento del rischio sono supportate da uno strumento realizzato in MS Excel che implementa il modello di seguito descritto, facilitandone l'applicazione.

6.1 Definizione del contesto

La definizione del contesto presenta l'insieme delle informazioni necessarie per descrivere:

- l'ambito di operatività e le sue variazioni;
- gli obiettivi;
- il livello di propensione del rischio dell'Ente;
- i fattori interni ed esterni che possono influenzare il processo di Risk Management;
- la tassonomia dei rischi, che include le categorie di rischio da considerare;
- le tecniche e gli strumenti di valutazione del rischio utilizzati;

- le responsabilità e le attività di reporting del processo di Risk Management.

Il contesto di riferimento per la valutazione del rischio cyber è desunto dal PIAO 2026-2028 della Regione Piemonte, quale documento unico di pianificazione e governance triennale dell'Ente, aggiornato annualmente.
La Regione opera su ambiti istituzionali eterogenei e ad elevato impatto pubblico, tra cui sanità, ambiente e territorio, mobilità, sviluppo, istruzione, politiche sociali, tributi, fondi europei e supporto agli enti territoriali.
Tale ampiezza funzionale comporta una forte dipendenza dalla continuità, integrità e disponibilità dei servizi digitali e dei dati trattati.
Il contesto così definito costituisce quindi il riferimento per calibrare impatti, priorità e soglie di accettabilità del rischio, in coerenza con il ruolo istituzionale dell'Ente e con la necessità di garantire servizi pubblici affidabili verso cittadini, imprese e altri enti.

6.2 Valutazione del Rischio (Risk Assessment)

Identificazione dei Rischi

Il Referente per la cybersicurezza e i Risk Owner, con il contributo delle strutture competenti e degli eventuali soggetti di supporto individuati in relazione allo specifico ambito di valutazione, identificano le minacce da portare in valutazione, tenendo in considerazione:

- gli obiettivi e i fattori rilevanti per l'Ente;
- le indicazioni delle normative, cogenti e volontarie (es. Direttiva NIS2, ISO 27001, CSA Star ecc.);
- l'assessment dei rischi dell'Ente;
- gli asset da proteggere.

L'identificazione delle minacce è effettuata considerando le minacce interne ed esterne, le vulnerabilità non risolte e gli impatti conseguenti ad eventuali incidenti.[2]

Il *risk register* così ottenuto è la base di partenza per la valutazione dei rischi.

Almeno ogni due anni, i risk owner verificano la corretta gestione dei rischi, dei controlli e dei presidi in essere e verificano la completezza del *risk register*. Ad ogni cambiamento di contesto i risk owner valutano la necessità di introdurre nel risk register nuove minacce o pericoli da portare in valutazione.[3]

Sono identificate inoltre le minacce e i rischi connessi alla sicurezza dei sistemi informativi e di rete, anche con riferimento alle eventuali dipendenze da fornitori e partner terzi[4].

L'identificazione del rischio associato alle forniture con impatto sulla sicurezza avviene considerando almeno i seguenti elementi[5]:
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;

[2] rif. requisito ID.RA-05 punto 4

[3] rif. requisito ID.RA-05 punto 2

[4] rif. requisito ID.RA-05 punto 1

[5] rif. requisito GV.SC-07 punto 1

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.

Analisi dei rischi

Al termine del processo di identificazione, i risk owner valutano il rischio inerente collegato alle singole minacce, ovvero il danno potenziale in assenza di presidi. Il rischio è valutato stimando probabilità (o verosimiglianza) di accadimento e impatto derivante dal rischio.

La tecnica utilizzata per la valutazione prevede il ricorso a metodi quantitativi e qualitativi. La **probabilità** e l'**impatto** sono entrambi valutati secondo una scala da 1 a 4.

Ciascun valore della scala è attribuito dal Risk Owner sulla base dei criteri di riferimento definiti nelle tabelle seguenti e delle informazioni disponibili sullo specifico scenario, al fine di rendere la valutazione quanto più possibile omogenea, motivata e ripetibile. Quando più dimensioni di impatto risultano interessate, la valutazione considera quella maggiormente rappresentativa delle conseguenze dello scenario secondo le regole implementate nello strumento di valutazione.

Probabilità/ verosimiglianza	Livello	Criterio connesso alla possibilità	Criterio probabilistico	Serie storiche
4	Quasi certo	È quasi certo che l'evento possa verificarsi nei prossimi 3 anni e la probabilità è così alta che potrebbe verificarsi già entro il prossimo anno (es. furto nei supermercati; attacco cyber ad aziende con dati ritenuti di valore).	Probabilità > 60% nei prossimi 3 anni	L'evento si è verificato oltre le 5 volte negli ultimi 5 anni o più di 2 volte nell'ultimo anno.
3	Probabile	È probabile il verificarsi dell'evento nei prossimi 3 anni e l'occorrere di tale evento è prevedibile secondo le fonti di informazione disponibili (es. aumento dei costi dell'energia a fronte di conflitti in determinate aree del mondo)	30% < Prob < 60% nei prossimi 3 anni	L'evento si è verificato da 4 a 5 volte negli ultimi 5 anni.
2	Possibile	È possibile il verificarsi dell'evento nei prossimi 3 anni e l'occorrere di tale evento non susciterebbe sorpresa (es. terremoto in aree considerate significativamente sismiche)	10% < Prob < 30% nei prossimi 3 anni	L'evento si è verificato da 2 a 3 volte negli ultimi 3 anni
1	Improbabile	È improbabile che possa verificarsi, se non in condizioni straordinarie ad oggi imprevedibili (es. alluvione in sito lontano da corsi d'acqua)	0% < Prob <10% nei prossimi 3 anni	L'evento si è verificato non più di 1 volta negli ultimi 5 anni.

Tabella 1 – Criteri valutazione probabilità

La valutazione dell'impatto economico considera gli effetti finanziari diretti e indiretti che il verificarsi dello scenario può determinare per l'Ente. Sono considerati, ove pertinenti, i costi necessari per la gestione e il ripristino dell'evento, l'acquisizione di beni o servizi straordinari, il ricorso a supporto specialistico, la ricostituzione o sostituzione di risorse compromesse, nonché ulteriori oneri economici ragionevolmente riconducibili allo scenario.

La classificazione è effettuata secondo una valutazione proporzionata alla rilevanza economica dell'impatto per l'Ente

La valutazione del livello di servizio è riferita alla capacità dell'Ente di garantire la continuità e regolarità dei servizi pubblici. L'impatto viene quindi classificato in base all'eventuale interruzione, degrado o turbamento delle funzioni istituzionali verso cittadini, imprese e altri enti.

La disponibilità del dato è valutata in base alla sua necessità per garantire la continuità dei servizi istituzionali e dei procedimenti amministrativi. L'impatto cresce quando l'indisponibilità del dato compromette

l'erogazione di servizi verso cittadini, imprese o altri enti, soprattutto se genera effetti a cascata su servizi o sistemi interdipendenti.

		Economico	Compliance	Reputazionale	Livello di Servizio	Sicurezza del dato e delle informazioni		
Impatto	**Livello**					**Integrità**	**Disponibilità**	**Riservatezza**
4	Critico	Impatto economico molto rilevante per l'Ente, tale da richiedere interventi straordinari significativi, riallocazioni rilevanti di risorse o l'attivazione di misure eccezionali per sostenere i costi derivanti dall'evento e dal relativo ripristino.	Violazione grave degli obblighi NIS / D.Lgs. 138/2024, relativa a governance, misure di gestione del rischio, notifica degli incidenti o inottemperanza a prescrizioni dell'Autorità competente, con possibile applicazione di sanzioni, responsabilità dirigenziali, disciplinari o amministrativo-contabili e impatto rilevante sulla continuità di funzioni istituzionali o servizi pubblici.	Danno d'immagine con esposizione mediatica nazionale, sovraregionale o comunque di particolare rilievo istituzionale, con perdita significativa di fiducia da parte di cittadini, imprese, utenti, altri enti o stakeholder istituzionali.	L'evento determina o può determinare l'interruzione o una grave perturbazione di un servizio pubblico o di una funzione istituzionale critica, con impatto significativo su cittadini, imprese, altri enti o servizi correlati.	La perdita di integrità riguarda dati autoritativi, certificativi, contabili, sanitari, assistenziali o comunque utilizzati per adottare provvedimenti, pagamenti, autorizzazioni, graduatorie, controlli, sanzioni o decisioni con effetti diretti su cittadini, imprese o altri enti. L'alterazione può produrre atti illegittimi, erogazioni indebite, dinieghi impropri, effetti su diritti/interessi o grave compromissione del servizio.	L'indisponibilità dei dati impedisce o può impedire l'erogazione di servizi istituzionali critici o essenziali, con effetti rilevanti su cittadini, imprese, altri enti o servizi correlati, oppure con possibile effetto domino su procedimenti e sistemi interdipendenti. Può configurare una grave perturbazione operativa dei servizi.	La divulgazione non autorizzata riguarda categorie particolari di dati personali, dati sanitari, genetici, biometrici, giudiziari, dati di minori o soggetti vulnerabili, oppure informazioni la cui esposizione può compromettere sicurezza dell'Ente, sicurezza pubblica, infrastrutture, credenziali, architetture, vulnerabilità, indagini o funzioni istituzionali critiche. L'impatto può essere grave o difficilmente reversibile su diritti, libertà, sicurezza o affidabilità dell'azione amministrativa.
3	Alto	Impatto economico rilevante, con costi non ordinari significativi per gestione, mitigazione e ripristino dell'evento, tali da richiedere specifica pianificazione o riallocazione di risorse.	Violazione rilevante degli obblighi NIS / D.Lgs. 138/2024, con carenze significative in documentazione, approvazione, attuazione o monitoraggio delle misure, gestione del rischio, gestione incidenti, fornitori o comunicazioni dovute, con possibile attivazione di rilievi, prescrizioni, verifiche, piani correttivi o sanzioni.	Danno d'immagine con esposizione mediatica regionale, territoriale ampia o settoriale rilevante, ovvero con contestazioni pubbliche da parte di utenti, enti, associazioni, organi di controllo o stakeholder istituzionali.	L'evento determina un grave degrado del servizio, con rischio di mancato rispetto di obblighi amministrativi, termini procedimentali, standard di qualità o livelli di servizio dichiarati dall'Ente.	La perdita di integrità riguarda dati rilevanti per procedimenti amministrativi, rendicontazioni, adempimenti normativi, rapporti con altri enti o processi istituzionali significativi. L'alterazione può produrre errori amministrativi rilevanti, rettifiche formali, ritardi procedimentali, contestazioni o necessità di bonifica strutturata dei dati.	L'indisponibilità dei dati impedisce o degrada in modo significativo l'erogazione di un servizio pubblico o di una funzione amministrativa rilevante, senza effetto domino generalizzato ma con impatto apprezzabile su utenti, uffici, procedimenti o obblighi istituzionali.	La divulgazione riguarda dati personali ordinari in quantità significativa, dati economici, patrimoniali, fiscali, lavorativi, procedimentali o informazioni amministrative riservate non ancora pubblicabili. L'evento può generare reclami, contenzioso, danno reputazionale, contestazioni, obblighi di notifica, perdita di fiducia o compromissione di procedimenti amministrativi.
2	Medio	Impatto economico contenuto ma apprezzabile, gestibile mediante le risorse disponibili nell'ambito dell'ordinaria programmazione o mediante limitati interventi correttivi e riallocazioni.	Non conformità parziale a requisiti normativi, misure, procedure o obblighi documentali NIS, senza compromissione grave dei servizi o degli obblighi essenziali di notifica, gestibile tramite integrazioni documentali, aggiornamenti, azioni correttive pianificate o rilievi di audit.	Danno d'immagine con esposizione locale, settoriale o temporalmente limitata, con contestazioni circoscritte da parte di utenti, uffici, categorie di destinatari o stakeholder.	L'evento determina un disservizio circoscritto, limitato a specifici uffici, procedimenti o categorie di utenti, gestibile tramite procedure alternative o workaround temporanei.	La perdita di integrità riguarda dati operativi o di supporto, con impatto circoscritto a specifici uffici, attività interne o procedimenti non critici. L'alterazione è recuperabile tramite controlli, riconciliazioni o correzioni puntuali, senza effetti sostanziali verso l'esterno.	L'indisponibilità dei dati determina un disservizio circoscritto, limitato a specifici uffici, procedimenti, basi dati o categorie di utenti, gestibile tramite procedure alternative, copie, estrazioni, sistemi secondari o workaround temporanei.	La divulgazione riguarda informazioni interne o dati personali limitati, non appartenenti a categorie particolari, con impatto circoscritto e gestibile tramite oscuramento, comunicazioni, rettifiche, misure correttive o limitata attività di gestione dell'incidente. Non compromette in modo significativo diritti degli interessati o funzioni istituzionali.
1	Basso	Impatto economico limitato o	Scostamento limitato da policy, procedure	Danno d'immagine moderato, prevalentemente	L'evento non determina interruzioni o	La perdita di integrità riguarda dati non autoritativi, non utilizzati per decisioni	L'indisponibilità dei dati riguarda informazioni non critiche o non necessarie	La divulgazione riguarda dati o informazioni già pubbliche, pubblicabili, anonimizzate,

		trascurabile, assorbibile nell'ambito della gestione ordinaria senza necessità di interventi finanziari significativi o specifiche riallocazioni di risorse.	interne, standard o prassi operative adottate per l'attuazione degli obblighi NIS, senza rilievi esterni significativi e gestibile con azioni correttive ordinarie o aggiornamenti documentali.	interno o limitato a segnalazioni puntuali, senza significativa esposizione pubblica o perdita apprezzabile di fiducia istituzionale.	degradi apprezzabili dei servizi verso l'esterno e non incide su termini, obblighi o standard di qualità dell'Ente.	amministrative, provvedimenti, pagamenti o servizi verso l'esterno. L'errore è facilmente individuabile e correggibile, con impatto trascurabile sull'azione amministrativa.	all'erogazione immediata di servizi verso l'esterno; l'impatto è interno, temporaneo e non compromette termini, obblighi o continuità dell'azione amministrativa.	aggregate o prive di elementi idonei a produrre effetti rilevanti su interessati, procedimenti, sicurezza o reputazione dell'Ente.

Tabella 2 – Criteri valutazione impatto

Il rischio, determinato dal prodotto della probabilità per l'impatto può quindi assumere i valori compresi in una matrice 4X4.

Calcolato il rischio inerente, il risk owner valuta la capacità dei presidi e dei controlli in essere, se presenti, di ridurre il livello di impatto e/o la probabilità di accadimento del rischio.

A ciascun presidio il risk owner assegnerà un valore di efficacia[6] in base ai criteri definiti nella tabella seguente.

Se il presidio opera in prevenzione il coefficiente di mitigazione andrà a diminuire la probabilità, se opera in contenimento, diminuirà l'impatto.

Efficacia delle misure		Range medio di mitigazione	Coefficiente di mitigazione	Criterio
Molto efficace (strutturato)	**4**	3,5 - 4	0,9	La misura si dimostra di assoluta e comprovata efficacia, tale da ridurre in maniera consistente e definitiva la minaccia. Tale risultato può essere desunto in virtù di incident occorsi, nell'adozione di tale misura, all'ente o a realtà terze in virtù di dati storici, oppure in ragione di valutazioni empiriche.
Efficace (Definito)	**3**	2,5 - 3,49	0,75	La misura si dimostra efficace e capace di ridurre in maniera significativa la minaccia, seppur in maniera non del tutto risolutiva. Tale risultato può essere desunto in virtù di incident occorsi, nell'adozione di tale misura, all'ente o a realtà terze in virtù di dati storici, oppure in ragione di valutazioni empiriche.
Parzialmente efficace (Basato su prassi)	**2**	2,0 - 2,49	0,5	La misura dimostra un certo grado di efficacia ma non tale da garantire un presidio puntuale della minaccia, la quale continua a presentare punti di significativa vulnerabilità. Tale risultato può essere desunto in virtù di incident occorsi, nell'adozione di tale misura, all'ente o a realtà terze in virtù di dati storici, oppure in ragione di valutazioni empiriche.
Poco efficace (Iniziale)	**1**	1,0 - 1,99	0,25	La misura si è dimostrata poco efficace a contenere la minaccia, o la sua efficacia non è dimostrata / dimostrabile sulla base dei dati storici e/o per via empirica o dovuta all'applicazione in contesti simili, anche presso realtà terze.

Tabella 3 – Criteri valutazione efficacia dei presidi

[6] rif. requisito ID.IM-01 punto 3

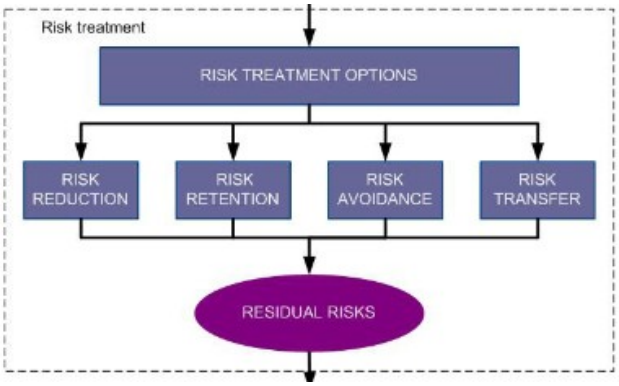
Il prodotto dato dai nuovi valori di impatto e probabilità costituirà il rischio "attuale".

Ponderazione dei rischi

Il valore del rischio attuale sarà compreso tra 1 e 16. In base al valore ottenuto e alle regole di ponderazione ovvero al "risk appetite" si deciderà la strategia di trattamento del rischio.

Il rischio potrà essere:

- Evitato, eliminando la causa, ad esempio rinunciando all'obiettivo connesso
- Trasferito a terzi, ad esempio ad un fornitore o ad una compagnia assicurativa
- Ritenuto, ovvero il suo impatto considerato sopportabile
- Mitigato, attraverso un'azione di trattamento che vada a ridurre la probabilità, agendo in prevenzione del danno o l'impatto, agendo in contenimento del danno.



Le strategie di gestione del rischio, le soglie di accettabilità e le priorità di intervento sono definite nell'ambito del processo di gestione del rischio, con il coordinamento del Settore A1911A – Sistema informativo regionale e il coinvolgimento del Referente per la cybersicurezza, dei Risk Owner e delle strutture competenti; gli esiti sono sottoposti al Comitato di coordinamento direttori ai fini del raccordo interdirezionale, secondo l'assetto organizzativo definito nel REGP_POL01.Il *risk appetite* è definito dalla quantità di rischi che l'Ente ritiene di poter sopportare.

Se la valutazione del rischio evidenzia un livello di rischio superiore al *risk appetite*, l'owner del rischio individuerà e assegnerà le azioni di trattamento da eseguire per diminuire il rischio.

A supporto delle decisioni è stata definita una matrice di tolleranza al rischio (Risk Appetite Framework).

Per tutti i rischi che superano il *risk appetite* sarà necessario definire e attuare azioni di mitigazione la cui priorità di intervento sarà definita dalla stessa matrice RAF (Risk Appetite Framework) di seguito rappresentata:

Probabilità/Impatto	Basso: 1	Medio: 2	Alto: 3	Critico: 4

Raro: 1	Risk Acceptance	Risk Acceptance	Risk Tolerance	Risk Capacity
Improbabile: 2	Risk Acceptance	Risk Tolerance	Risk Tolerance	Risk Capacity
Probabile: 3	Risk Acceptance	Risk Tolerance	Risk Capacity	Out of risk
Quasi certo: 4	Risk Acceptance	Risk Capacity	Out of risk	Very critical

Tabella 4 – Risk Appetite Framework

Priorità	livello di rischio	Azioni di mitigazione e controllo
1	Very critical	da implementare entro 1 mese
2	Out of risk	da implementare entro 3 mesi
3	Risk Capacity	da implementare entro 6 mesi
4	Risk Tolerance	da implementare entro 1 anno
5	Risk Acceptance	non richieste

Tabella 5 – Priorità di intervento

Nei casi in cui le tempistiche prescritte non fossero compatibili con i tempi di attuazione delle azioni di trattamento sarà necessario provvedere alla realizzazione di una soluzione workaround che possa mitigare il rischio nella fase di attuazione.

Nei casi in cui non fosse possibile un workaround, il risk owner dovrà richiedere una deroga rispetto ai tempi di intervento.

6.3 ESITI DELLE VALUTAZIONI DEL RISCHIO

In applicazione della metodologia descritta nel presente documento, Regione Piemonte ha effettuato una valutazione trasversale dei rischi cyber dell'Ente e specifiche valutazioni riferite ai sistemi informativi e di rete rilevanti individuati.

La valutazione complessiva considera gli scenari di rischio trasversali riferiti al contesto organizzativo, tecnologico e operativo della Regione. Le valutazioni riferite ai singoli sistemi informativi e di rete rilevanti approfondiscono invece l'esposizione allo specifico contesto di servizio, tenendo conto delle caratteristiche del sistema, delle informazioni trattate, delle dipendenze, dell'esposizione alle minacce e dei presidi esistenti.

Le due tipologie di valutazione hanno pertanto finalità complementari e differenti livelli di analisi; i relativi risultati non sono sommati o aggregati come se appartenessero a un unico insieme omogeneo di scenari.

Il presente documento ne riporta una sintesi finalizzata a rappresentare il profilo di rischio dell'Ente e dei sistemi informativi e di rete rilevanti. Il dettaglio delle singole valutazioni, dei parametri utilizzati, dei presidi considerati e dei valori attribuiti è mantenuto negli strumenti operativi di valutazione del rischio adottati dall'Ente.

Riepilogo degli esiti delle valutazioni

Assessment	Ambito	Scenari	Rischio inerente	Rischio attuale

		valutati		
REGP_RSK01	Regione Piemonte – valutazione complessiva	57	2 Risk Acceptance; 11 Risk Tolerance; 14 Risk Capacity; 25 Out of Risk; 5 Very Critical	**52 Risk Acceptance; 5 Risk Tolerance**
REGP_RSK02	Sala operativa Protezione Civile	9	4 Risk Tolerance; 2 Risk Capacity; 3 Out of Risk	**8 Risk Acceptance; 1 Risk Tolerance**
REGP_RSK03	Fascicolo Sanitario Elettronico	9	1 Risk Tolerance; 4 Risk Capacity; 1 Out of Risk; 3 Very Critical	**6 Risk Acceptance; 3 Risk Tolerance**
REGP_RSK04	Sito istituzionale	9	4 Risk Tolerance; 4 Risk Capacity; 1 Out of Risk	**8 Risk Acceptance; 1 Risk Tolerance**
REGP_RSK05	Rete di Palazzo	9	Tutti gli scenari in Risk Acceptance	**9 Risk Acceptance**

La tabella riporta esclusivamente una rappresentazione sintetica degli esiti delle valutazioni effettuate. Per gli scenari il cui livello di rischio attuale risulta superiore alla soglia di Risk Acceptance viene data evidenza del livello rilevato, senza riportare nel presente documento le successive decisioni di trattamento, le azioni, le responsabilità, le tempistiche o il rischio residuo atteso, che appartengono al distinto processo di trattamento del rischio.

Gli esiti mostrano che, tenuto conto dei presidi e dei controlli già attuati, la maggior parte degli scenari valutati presenta un livello di rischio attuale ricompreso nella classe Risk Acceptance. Permangono alcuni scenari classificati Risk Tolerance, che costituiscono elementi di ingresso per il successivo processo di trattamento del rischio.

È stata valutata anche l'infrastruttura della rete di palazzo: l'eventuale indisponibilità dell'infrastruttura di rete della sede determina l'impossibilità o una significativa limitazione dell'operatività dalla sede interessata, senza tuttavia comportare di per sé l'indisponibilità dei servizi informativi regionali, ospitati presso infrastrutture esterne alla sede. Per le attività compatibili, la continuità operativa può essere assicurata mediante lavoro da remoto. La probabilità di indisponibilità è inoltre mitigata dalla ridondanza dei collegamenti e degli apparati principali, dalla segmentazione dell'infrastruttura, dal monitoraggio centralizzato e dal presidio tecnico presente presso la sede. Pertanto, non vi sono rischi da mitigare.

Le valutazioni sono soggette a riesame periodico e possono essere aggiornate in relazione a variazioni del contesto, delle minacce, delle vulnerabilità, dei sistemi e servizi interessati o dell'efficacia dei presidi esistenti. Il dettaglio analitico e aggiornato delle valutazioni è mantenuto negli strumenti operativi adottati dall'Ente.

6.4 TRATTAMENTO DEI RISCHI[7]

Successivamente alla ponderazione viene redatto il Piano di trattamento dei rischi nel quale devono essere evidenziate le opzioni di trattamento e le relative priorità secondo quanto riportato nel paragrafo precedente (eliminazione, trasferimento, riduzione, accettazione).

[7] rif. requisito ID.RA-06 punto 1

Il Piano prevede che ad ogni azione individuata sia assegnata la responsabilità in merito all'attuazione (action owner) e sia pianificata una data per il completamento. Deve inoltre essere stimato il valore del rischio residuo atteso al completamento dell'azione di trattamento e deve essere data indicazione delle motivazioni di accettazione del rischio, laddove questo superi le soglie di accettabilità.

Successivamente alla ponderazione del rischio, gli scenari che richiedono interventi di trattamento sono riportati nel Piano di trattamento dei rischi, nel quale sono indicate le opzioni di trattamento individuate, le priorità, le azioni previste, i soggetti responsabili dell'attuazione e le relative tempistiche.

Il Piano di trattamento è predisposto con il coinvolgimento delle strutture responsabili dei servizi, dei sistemi, dei processi o degli ambiti interessati, secondo l'assetto organizzativo definito dall'Ente e richiamato nel documento REGP_POL01.

L'eventuale accettazione del rischio residuo è motivata, documentata e sottoposta alla sede decisionale competente secondo l'assetto organizzativo dell'Ente, ferma restando la necessità di approvazione da parte dei vertici dell'Ente nei casi previsti dalla normativa o dalle specifiche applicabili.

L'avanzamento delle azioni di trattamento è monitorato secondo le modalità definite nel Piano di trattamento dei rischi e negli strumenti operativi di supporto.

6.4.1 Deroghe[8]

Qualora, per motivate e documentate ragioni normative, tecniche od organizzative, non sia possibile attuare nei tempi previsti una misura o un requisito applicabile, l'Ente registra tale circostanza nello strumento operativo pertinente o nel Piano di trattamento dei rischi.

La registrazione della deroga o del differimento deve indicare almeno: la misura o il requisito interessato, la motivazione, le misure compensative o temporanee adottate, il rischio residuo, il soggetto responsabile, la data prevista di riesame e l'eventuale sede decisionale competente per la validazione.

Le deroghe non comportano l'esclusione del rischio dal processo di gestione, ma ne richiedono la tracciabilità, il monitoraggio e il riesame periodico.

6.5 Monitoraggio e Riesame

Il monitoraggio e il riesame sono svolti secondo l'assetto organizzativo definito dall'Ente e richiamato nel documento REGP_POL01, con il coinvolgimento delle strutture responsabili dei rischi, delle azioni di trattamento e dei sistemi o servizi interessati.

L'attività di monitoraggio e riesame riguarda tutte le fasi del processo di gestione del rischio cyber ed è finalizzata a verificare:

- l'eventuale variazione del contesto, delle minacce, delle vulnerabilità o dell'esposizione al rischio;
- lo stato di avanzamento delle azioni di trattamento;
- l'adeguatezza delle misure già adottate;
- l'eventuale necessità di aggiornare il registro dei rischi, il piano di trattamento o le priorità di intervento;
- la corretta conservazione delle evidenze documentali a supporto delle valutazioni effettuate.

[8] Rif.ID.RA-06 punto 2

Le strutture responsabili dei servizi, dei sistemi, dei processi o degli ambiti interessati comunicano tempestivamente alla funzione di coordinamento del processo eventuali variazioni rilevanti, criticità attuative, ritardi o necessità di rivalutazione del rischio.

6.6 COMUNICAZIONE E CONSULTAZIONE

Il presente documento è reso disponibile alle strutture e ai soggetti coinvolti nel processo di gestione del rischio cyber secondo le modalità di pubblicazione, diffusione e accesso definite dall'Ente.

Gli esiti delle valutazioni del rischio, lo stato di avanzamento delle azioni di trattamento e le eventuali criticità rilevanti sono comunicati alle strutture competenti e, ove necessario, agli organi di amministrazione e direttivi, secondo i flussi informativi previsti dal documento REGP_POL01 e dagli strumenti operativi di supporto.

La comunicazione degli esiti avviene nel rispetto delle esigenze di riservatezza, sicurezza delle informazioni e necessità di conoscenza.

Regione Piemonte

PIANO DI TRATTAMENTO DEI RISCHI PER LA SICUREZZA INFORMATICA

Versione	Data	Descrizione	Redazione	Approvazione
V01	[gg/mm/aaaa]	Prima versione del Piano di trattamento dei rischi per la sicurezza informatica	[struttura/ruolo]	[organo/figura competente]

Sommario

1 Finalità del documento....3
2 Ambito di applicazione....3
3 Criteri di compilazione e aggiornamento....3
4 Piano di trattamento del rischio....4
4.1 Rischi complessivi dell'Ente....4
4.2 Rischi per la Sala Operativa....5
4.3 Rischi per il Fascicolo Sanitario Elettronico....5
4.4 Rischi per il sito....5
4.5 Rischi per la rete di palazzo....5
5 Validazione, monitoraggio e aggiornamento....5

1 Finalità del documento

Il presente Piano documenta le scelte operate da Regione Piemonte in merito al trattamento dei rischi individuati e ponderati nell'ambito del processo di valutazione del rischio cyber.

Il documento costituisce il riferimento consolidato per la definizione delle strategie e delle priorità di trattamento e, per i rischi che richiedono specifici interventi, delle azioni pianificate, delle responsabilità e delle relative tempistiche di attuazione. Per i rischi per i quali è adottata una strategia di accettazione, il Piano assicura il raccordo con le valutazioni analitiche nelle quali sono mantenuti il livello di rischio e le motivazioni della relativa decisione.

Il Piano costituisce evidenza documentale dell'attuazione del processo di trattamento del rischio ed è redatto in coerenza con il REGP_PIA03 – Valutazione del rischio cyber e con l'assetto organizzativo descritto nel REGP_POL01 – Organizzazione per la sicurezza informatica.

2 Ambito di applicazione

Il Piano si applica ai rischi informatici individuati e ponderati nell'ambito delle valutazioni del rischio effettuate dall'Ente, sia a livello complessivo sia con riferimento ai sistemi informativi e di rete rilevanti sottoposti a specifico assessment.

Il Piano utilizza gli esiti delle valutazioni come elemento di ingresso del processo di trattamento, evitando di replicare il dettaglio analitico delle minacce, delle vulnerabilità, dei presidi e dei calcoli mantenuto negli strumenti operativi di valutazione del rischio.

Le valutazioni REGP_RSK costituiscono pertanto la fonte analitica del livello di rischio e delle informazioni utilizzate per le decisioni di trattamento. Il presente Piano ne consolida le decisioni, le priorità e gli eventuali interventi conseguenti, mantenendo un riferimento univoco allo scenario di rischio cui ciascuna decisione si riferisce.

I ruoli, le responsabilità e i raccordi organizzativi rilevanti ai fini della predisposizione, approvazione, attuazione e monitoraggio del presente Piano sono quelli definiti nel REGP_POL01 – Organizzazione per la sicurezza informatica e negli ulteriori atti organizzativi vigenti dell'Ente.

3 Criteri di compilazione e aggiornamento

Il Piano è alimentato a partire dagli esiti delle valutazioni del rischio cyber dell'Ente, documentate nei relativi assessment REGP_RSK.

Le valutazioni di riferimento costituiscono la fonte analitica delle informazioni relative agli scenari di rischio, al livello e alla priorità del rischio, alla strategia di trattamento adottata, al rischio residuo pianificato e agli ulteriori elementi utilizzati a supporto delle decisioni di trattamento.

Al fine di evitare duplicazioni e mantenere il presente documento sintetico e orientato al monitoraggio degli interventi, nelle tabelle del Piano sono riportate esclusivamente le informazioni di maggiore interesse ai fini dell'attuazione del trattamento, quali:

- lo scenario o la minaccia cui l'intervento si riferisce;
- l'azione o gli interventi pianificati;
- il soggetto responsabile dell'attuazione;
- la data prevista di completamento;

· le motivazioni o gli elementi sintetici utili a descrivere l'intervento.

Le informazioni analitiche relative alla valutazione del rischio e alla decisione di trattamento restano documentate nei rispettivi assessment REGP_RSK, ai quali le sezioni del presente Piano fanno riferimento. Eventuali aggiornamenti della valutazione che comportino modifiche delle decisioni o delle azioni di trattamento determinano il conseguente aggiornamento del presente Piano.

Per gli scenari il cui rischio ricade nei criteri di accettazione definiti dalla metodologia dell'Ente e per i quali non sono previste specifiche azioni di trattamento, le relative valutazioni e decisioni rimangono documentate negli assessment REGP_RSK di riferimento e non sono duplicate nelle tabelle del presente Piano.

Ai fini dell'approvazione del Piano deve tuttavia essere assicurata la tracciabilità dei rischi oggetto di accettazione e delle relative decisioni, secondo quanto previsto dal processo di gestione del rischio dell'Ente e dalla disciplina applicabile.

Il documento è aggiornato a seguito di:

- revisione della valutazione del rischio con la conseguente variazione dei trattamenti;
- modifiche rilevanti ai sistemi, ai servizi o al contesto organizzativo;
- variazioni delle minacce, delle vulnerabilità o dell'esposizione al rischio;
- completamento, revisione o superamento degli interventi previsti;
- riesame periodico del rischio informatico (almeno ogni due anni).

4 Piano di trattamento del rischio

Le sezioni seguenti riportano il piano consolidato di trattamento dei rischi risultanti dalle valutazioni effettuate dall'Ente. I trattamenti sono organizzati per ambito di valutazione, mantenendo il raccordo con gli esiti del processo di valutazione del rischio senza duplicarne il dettaglio analitico.

4.1 Rischi complessivi dell'Ente

Minaccia/Pericolo	Azioni	Responsabile azione	Data fine prevista	Motivazione azione
Compromissione della manutenibilità del sistema informativo	Piani Cloud di adeguamento applicativo (Allegati 2 e 3)	Direzione / Settore regionale titolare del processo, servizio o banca dati	31/12/2027	Al fine di adeguare il parco applicativo regionale alle normative Cloud l'Ente ha avviato un piano di adeguamento applicativo
Ingegneria sociale	Programma di formazione e simulazione sul phishing e sull'ingegneria sociale rivolto al personale regionale	A1911A Sistema informativo regionale	31/12/2026	All'interno dell'intervento su Misura 55 sarà finanziata la formazione al personale regionale sul rischio di ingegneria sociale
Furto di apparecchiature	Adozione di una soluzione centralizzata per la gestione e la protezione dei dispositivi mobili	A1911A Sistema informativo regionale	31/12/2026	In corrispondenza con la distribuzione dei nuovi dispositivi mobili necessari anche per la sicurizzazione tramite MFA sarà acquisito uno strumento per la gestione dei dispositivi mobili che andrà a mitigare il richio in oggetto

Furto di identità digitale o credenziali	Adozione MFA	A1911A Sistema informativo regionale	31/12/2026	L'ente ha investito nell'adozione di una soluzione MFA per proteggere le utenze dei dipendenti e contestualmente distribuito dispositivi portatili
Divulgazione non autorizzata di informazioni	Estensione della cifratura dei dischi alle postazioni di lavoro portatili	A1911A Sistema informativo regionale	31/12/2026	L'Ente utilizza PdL in RDS per cui il rischio potrebbe considerarsi basso, ma per la componente di parco notebook attivare la cifratura del disco potrebbe migliorare la postura complessiva

4.2 Rischi per la Sala Operativa

Minaccia/Pericolo	Azioni	Responsabile azione	Data fine prevista	Motivazione azione
Disponibilità	Predisposizione di un piano di continuità operativa per la sala	Direzione Opere Pubbliche, Difesa del Suolo, Protezione civile, Trasporti e Logistica	31/12/2026	Impostare un piano adeguato alle necessità della sala operativa

4.3 Rischi per il Fascicolo Sanitario Elettronico

Minaccia/Pericolo	Azioni	Responsabile azione	Data fine prevista	Motivazione azione
Integrità dei dati	Intervento pianificato con SAN_7_06 Evoluzione del Fascicolo Sanitario Elettronico- Intervento n. 6: Allestimento degli ambienti di disaster recovery	Direzione sanità	01/01/2027	Rendere più resiliente il servizio attraverso l'adizione di una soluzione di disaster recovery
Disponibilità	Intervento pianificato con SAN_7_06 Evoluzione del Fascicolo Sanitario Elettronico- Intervento n. 6: Allestimento degli ambienti di disaster recovery	Direzione sanità	01/01/2027	Rendere più resiliente il servizio attraverso l'adizione di una soluzione di disaster recovery
Supply chain / fornitore	Intervento pianificato con SAN_7_06 Evoluzione del Fascicolo Sanitario Elettronico- Intervento n. 6: Allestimento degli ambienti di disaster recovery	Direzione sanità	01/01/2027	Rendere più resiliente il servizio attraverso l'adizione di una soluzione di disaster recovery

4.4 Rischi per il sito

Minaccia/Pericolo	Azioni	Responsabile azione	Data fine prevista	Motivazione azione
Disponibilità	Migrazione del sito istituzionale verso	Settore A1911A – Sistema	31/12/2026	Ridurre il rischio di indisponibilità mediante il ricorso a

	l'ambiente cloud previsto dalla pianificazione regionale	informativo regionale		un'architettura con maggiori caratteristiche di resilienza e capacità di ripristino rispetto all'attuale soluzione, secondo quanto previsto dalla pianificazione di migrazione dell'Ente.

4.5 Rischi per la rete di palazzo

Per la rete di palazzo non sono emersi rischi da mitigare.

5 Validazione, monitoraggio e aggiornamento

Il Piano è predisposto con il coinvolgimento delle strutture responsabili dei rischi e dei soggetti responsabili delle azioni di trattamento, secondo l'assetto organizzativo definito nel REGP_POL01 – Organizzazione per la sicurezza informatica. Per i profili trasversali è sottoposto al Comitato di coordinamento direttori ai fini del raccordo interdirezionale e, secondo quanto previsto dalla disciplina applicabile e dall'assetto organizzativo dell'Ente, all'approvazione degli organi di amministrazione e direttivi competenti.

Gli interventi riportati nel Piano sono monitorati con riferimento allo stato di avanzamento, alle responsabilità assegnate, alle scadenze previste e alle eventuali variazioni delle condizioni di rischio.

Il livello di rischio residuo riportato nel Piano prima del completamento dell'intervento costituisce una stima pianificata. A conclusione del trattamento è effettuata una nuova valutazione dell'efficacia delle misure adottate e del rischio effettivamente residuo.

L'eventuale accettazione del rischio residuo è motivata e documentata ed è sottoposta all'approvazione secondo le competenze previste dall'assetto organizzativo dell'Ente e dalla disciplina applicabile.

Le modifiche al Piano possono derivare dal riesame delle valutazioni del rischio, dal completamento o dalla revisione degli interventi, da nuove decisioni di trattamento, da variazioni del contesto o da mutate condizioni di esposizione al rischio.

Allegato A – Fonti utilizzate

Il presente Piano è stato generato utilizzando i seguenti file di valutazione del rischio:

REGP_RSK01_CyberRisk_Assessment_v01

REGP_RSK02_CyberRisk_Assessment_SalaOp_v01

REGP_RSK03_CyberRisk_Assessment_fse_v01

REGP_RSK04_CyberRisk_Assessment_Sito_v01

REGP_RSK05_CyberRisk_Assessment_RetePal_v01

Regione Piemonte

PIANO DI ADEGUAMENTO

ai fini dell'attuazione delle politiche di sicurezza informatica

Versione	Data	Descrizione	Redazione	Approvazione
V01	[gg/mm/aaaa]	Prima emissione	[struttura/ruolo]	Organi di amministrazione e direttivi competenti

1 Sommario

2 Finalità e ambito del Piano....3
3 Base informativa del Piano e ciclo di aggiornamento....3
4 Sintesi dello stato di adeguamento dell'Ente....3
4.1 Esiti sintetici della gap analysis di riferimento....4
4.2 Principali esigenze di adeguamento rilevate....4
5 Criteri di individuazione e priorità delle azioni....5
6 Raccordo con il Piano di trattamento del rischio....5
7 Monitoraggio, aggiornamento e reporting....6
8 Registro operativo delle azioni di adeguamento....7
9 Sintesi delle azioni di adeguamento....8
10 Allegato 1 – REGP_REG03 - Registro operativo delle azioni di adeguamento....10

2 Finalità e ambito del Piano

Il presente Piano di adeguamento individua, in forma sintetica e programmatoria, le principali linee di intervento che Regione Piemonte intende realizzare per rafforzare il proprio assetto organizzativo, documentale, procedurale e operativo in materia di sicurezza informatica e per assicurare l'attuazione delle politiche, dei processi e delle misure di sicurezza applicabili all'Ente nell'ambito della disciplina NIS.

Il Piano è predisposto in attuazione della misura ID.IM-01 delle Linee guida NIS – Specifiche di base e, in particolare, tiene conto degli esiti del riesame delle politiche di sicurezza previsto dalla misura GV.PO-02 e delle ulteriori valutazioni ed evidenze disponibili, al fine di individuare gli interventi necessari ad assicurare l'attuazione e il miglioramento delle politiche e delle misure di sicurezza applicabili all'Ente.

Il Piano non sostituisce il Piano di trattamento del rischio, né replica al proprio interno le decisioni di trattamento dei rischi già formalizzate in tale documento. Il presente documento si concentra sugli adeguamenti organizzativi, documentali, procedurali e operativi derivanti dalla gap analysis, da verifiche, audit, vulnerabilità, incidenti, riesami, aggiornamenti normativi o variazioni del contesto organizzativo e tecnologico.

Il dettaglio operativo delle azioni è riportato nell'Allegato REGP_REG03 - Registro operativo delle azioni di adeguamento, che costituisce lo strumento di lavoro per monitorare avanzamento, priorità, scadenze, responsabilità, dipendenze ed evidenze di chiusura.

Le azioni riportate nel Piano possono avere natura diversa: alcune sono finalizzate al completamento dell'attuazione di requisiti normativi applicabili, altre al consolidamento di presidi già esistenti o al miglioramento progressivo della postura di sicurezza dell'Ente. Tale distinzione è considerata nella definizione delle priorità e delle scadenze e deve risultare tracciabile nel Registro operativo.

Il presente Piano è sottoposto all'approvazione degli organi di amministrazione e direttivi competenti secondo l'assetto organizzativo definito dall'Ente.

3 Base informativa del Piano e ciclo di aggiornamento

Il Piano è predisposto sulla base degli esiti della gap analysis vigente alla data di predisposizione, svolta con riferimento ai requisiti e alle misure applicabili all'Ente. La versione della gap analysis utilizzata quale base istruttoria è quella richiamata nella sezione 3.1.

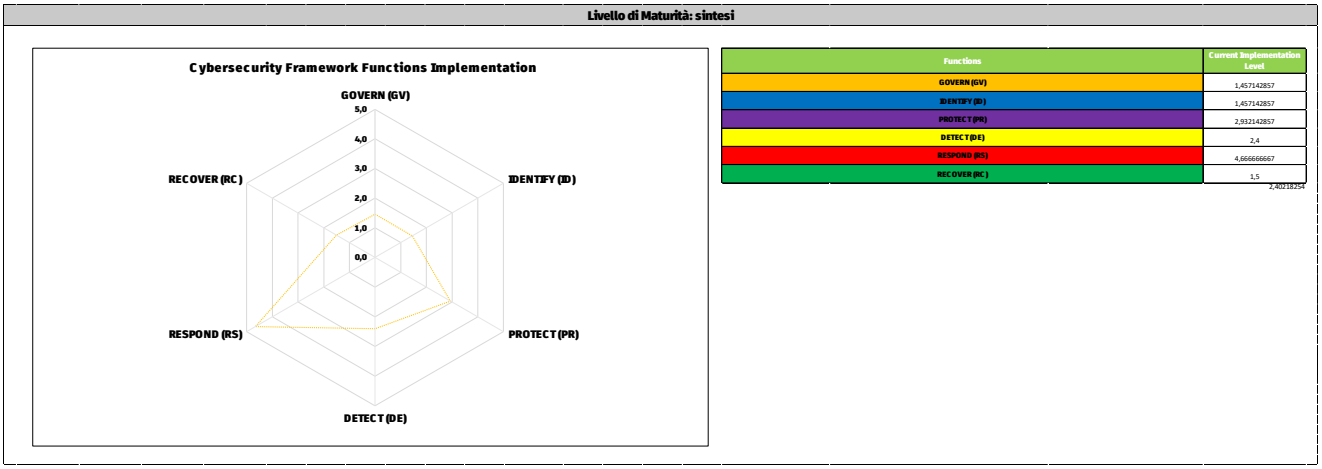
Il presente documento ne recepisce gli esiti in forma sintetica, al fine di rappresentare lo stato di adeguamento dell'Ente, individuare le principali esigenze di miglioramento e definire le linee di intervento da pianificare nel periodo di riferimento.

Lo stato e lo storico delle azioni mantenute nel Registro operativo costituiscono una delle fonti informative utilizzate per il successivo riesame della gap analysis, senza sostituirla. L'aggiornamento della gap analysis è svolto quale attività istruttoria distinta e concorre, insieme alle ulteriori evidenze disponibili, alla predisposizione e al riesame del Piano di adeguamento.

4 Sintesi dello stato di adeguamento dell'Ente

La presente sezione riporta una sintesi direzionale dello stato di adeguamento dell'Ente, sulla base della gap analysis aggiornata e delle ulteriori evidenze disponibili alla data di predisposizione del Piano.

4.1 Esiti sintetici della gap analysis di riferimento



Il quadro sintetico, riferito alla gap analysis REGP_NIS2 Assessment_v03 del 27/02/2026, evidenzia livelli di implementazione differenziati tra le funzioni considerate. I valori relativamente più contenuti riguardano le funzioni GOVERN, IDENTIFY e RECOVER, mentre la funzione RESPOND presenta il livello di implementazione più elevato. PROTECT e DETECT si collocano in una posizione intermedia.

Gli esiti della gap analysis costituiscono la base istruttoria iniziale del Piano e sono integrati dalle ulteriori evidenze e necessità di adeguamento emerse successivamente e registrate nel REGP_REG03. La rappresentazione sintetica non costituisce pertanto un'attestazione dello stato corrente di conformità né sostituisce la verifica puntuale dei singoli requisiti applicabili.

Fonte istruttoria: REGP_NIS2 Assessment_v03 - 27/02/2026

4.2 Principali esigenze di adeguamento rilevate

Sulla base della gap analysis e delle ulteriori esigenze recepite nel Registro operativo, le principali direttrici di adeguamento riguardano:

- il consolidamento dell'impianto organizzativo e documentale di sicurezza informatica, comprensivo dell'aggiornamento della gap analysis, del raccordo tra politiche, piani, procedure e registri e del relativo adeguamento all'evoluzione normativa;
- il completamento e il consolidamento delle informazioni necessarie all'identificazione e al governo del perimetro ICT, con particolare riferimento agli inventari di asset, software, servizi, servizi esternalizzati e flussi di rete;
- il rafforzamento della gestione delle vulnerabilità, attraverso la pianificazione delle attività di vulnerability assessment e penetration test, l'estensione degli strumenti di supporto e la progressiva razionalizzazione e messa in sicurezza del parco applicativo;
- il rafforzamento delle misure di protezione degli accessi e dei dispositivi, mediante interventi quali la cifratura delle postazioni portatili, la gestione centralizzata dei dispositivi mobili e l'evoluzione delle modalità di autenticazione;

- il consolidamento della gestione del rischio cyber nella catena di approvvigionamento e negli affidamenti ICT;
- il completamento e l'attuazione del sistema di continuità operativa, ripristino in caso di disastro e gestione delle crisi, incluse le relative attività di verifica ed esercitazione;
- il mantenimento di un programma strutturato e continuativo di formazione e consapevolezza in materia di sicurezza informatica.

Le singole azioni, le priorità, le strutture competenti, le scadenze e il relativo stato di avanzamento sono mantenuti nel REGP_REG03 – Registro operativo delle azioni di adeguamento.

5 Criteri di individuazione e priorità delle azioni

Le azioni inserite nel Registro operativo sono individuate e prioritizzate sulla base di criteri proporzionati al contesto organizzativo e tecnologico dell'Ente. La priorità non deriva esclusivamente dalla classificazione normativa del requisito, ma tiene conto anche dell'effetto atteso dell'intervento, della fattibilità attuativa e delle dipendenze organizzative o contrattuali.

Criterio	Descrizione	Uso nel Piano
Rilevanza per l'adeguamento	L'azione contribuisce a colmare gap, rafforzare evidenze, completare documenti, procedure o presidi organizzativi richiesti dall'impianto NIS applicabile.	Aiuta a distinguere le azioni necessarie da quelle meramente migliorative.
Impatto organizzativo-operativo	L'azione incide sulla capacità dell'Ente di governare processi, responsabilità, fornitori, evidenze o continuità delle attività.	Aiuta a individuare le azioni con maggiore valore per l'Ente.
Sostenibilità attuativa	L'azione è valutata rispetto a risorse disponibili, vincoli organizzativi, dipendenze da fornitori, tempi tecnici e impatti operativi.	Consente una roadmap realistica e attuabile per una PA.
Evidenziabilità	L'azione produce evidenze documentali, procedurali, tecniche o organizzative verificabili.	Supporta audit, riesami e reporting agli organi competenti.

Nel Registro operativo le azioni sono inoltre classificate mediante viste complementari, al fine di consentire sia la lettura gestionale sia il raccordo con i requisiti tecnici e documentali applicabili.

Vista di classificazione	Funzione	Esempi di valori
Origine dell'azione	Spiega perché l'azione è stata inserita nel Piano.	Gap analysis; vulnerabilità; incidente; audit interno; audit di certificazione; riesame; fornitore; aggiornamento normativo
Natura dell'intervento	Individua il tipo di attività richiesta.	Documentale; organizzativa; procedurale; tecnologica; contrattuale; formativa; verifica/test; remediation

6 Raccordo con il Piano di trattamento del rischio

Il Piano di adeguamento opera in coerenza con il Piano di trattamento del rischio, senza sostituirlo e senza duplicarne i contenuti. Il Piano di trattamento del rischio resta il documento nel quale sono descritte le scelte operate dall'Ente in merito ai rischi individuati, alle relative priorità di trattamento e all'eventuale rischio residuo accettato.

Il Registro operativo allegato al presente Piano non costituisce un secondo registro dei rischi e non ridefinisce le decisioni di trattamento formalizzate nel REGP_PIA04 – Piano di trattamento dei rischi per la sicurezza informatica.

Per esigenze di pianificazione e monitoraggio unitario dell'adeguamento, il REGP_REG03 può tuttavia ricomprendere anche interventi che costituiscono attuazione, totale o parziale, di decisioni di trattamento del rischio già formalizzate nel REGP_PIA04. In tali casi il Registro monitora esclusivamente gli aspetti attuativi dell'intervento, quali responsabilità, scadenze, stato di avanzamento ed evidenze di completamento, senza modificare la decisione di trattamento, la relativa motivazione o la valutazione del rischio.

Le ulteriori azioni del Registro possono derivare dalla gap analysis, da esigenze organizzative o tecnologiche, da vulnerabilità, incidenti, riesami, verifiche, rapporti con fornitori o aggiornamenti normativi e di contesto.

Il Piano di adeguamento raccoglie invece gli interventi di natura organizzativa, documentale, procedurale e operativa necessari a migliorare l'attuazione complessiva delle politiche e delle misure di sicurezza, sulla base della gap analysis aggiornata e delle ulteriori evidenze disponibili.

Qualora, durante l'attuazione del Piano di adeguamento, emergano elementi che possano incidere sulla valutazione dei rischi o sulle scelte di trattamento già assunte, tali elementi sono riportati al processo di aggiornamento della valutazione del rischio e del Piano di trattamento del rischio, secondo le modalità previste dall'Ente.

7 Monitoraggio, aggiornamento e reporting

Il monitoraggio dell'attuazione del Piano è effettuato mediante aggiornamento periodico del Registro operativo delle azioni di adeguamento. L'aggiornamento del Registro non comporta necessariamente la revisione formale del presente Piano, salvo modifiche sostanziali delle linee di adeguamento, delle priorità o dell'ambito di applicazione.

Il Registro è aggiornato con cadenza semestrale e comunque in occasione dell'emersione di nuovi gap, rischi, vulnerabilità, incidenti, risultanze di audit, riesami, modifiche organizzative o variazioni tecnologiche rilevanti.

Gli esiti dell'attuazione del Piano sono rappresentati mediante una sintesi periodica contenente almeno lo stato di avanzamento delle azioni, le azioni concluse, quelle scadute o bloccate e le principali criticità attuative.

La sintesi è sottoposta al Comitato di coordinamento direttori ai fini dell'esame e del raccordo interdirezionale e concorre all'informativa periodica agli organi di amministrazione e direttivi competenti prevista dalla disciplina applicabile. Eventuali decisioni necessarie sono sottoposte ai soggetti competenti secondo l'assetto organizzativo dell'Ente.

Indicatore	Descrizione	Uso nel reporting
Azioni aperte / chiuse	Numero complessivo e percentuale di avanzamento.	Misura l'attuazione generale del Piano.
Azioni ad alta priorità	Azioni con maggiore rilevanza per rischio, conformità o continuità.	Evidenzia le priorità direzionali.
Azioni scadute o bloccate	Azioni non completate nei tempi o dipendenti da vincoli esterni.	Richiede eventuali decisioni, ripianificazioni o escalation.

8 Registro operativo delle azioni di adeguamento

Il Registro operativo delle azioni di adeguamento costituisce l'unico allegato operativo al presente Piano. Esso contiene il dettaglio delle azioni pianificate, in corso, concluse, sospese, annullate o rinviate, nonché le informazioni necessarie al monitoraggio e alla verifica dell'attuazione.

Il Registro è gestito come strumento operativo aggiornabile. La sua struttura consente di mantenere nel documento principale una sintesi stabile e direzionale, evitando revisioni formali del Piano per ogni aggiornamento puntuale delle singole azioni.

Il Registro operativo costituisce l'evidenza analitica del Piano di adeguamento. Il presente documento può riportare una tabella di sintesi generata dal Registro operativo, limitata ai campi necessari alla lettura gestionale delle azioni. Il dettaglio completo resta contenuto nel Registro allegato, nelle relative viste di sintesi e nella dashboard in esso contenute.

Campo del Registro	Tipo	Descrizione
ID azione	Da compilare	Codice univoco dell'azione.
Titolo azione	Da compilare	Titolo breve dell'azione, utile per la lettura sintetica del registro.
Descrizione sintetica / criticità	Da compilare	Descrive il gap, la criticità, l'esigenza di miglioramento o l'intervento da realizzare.
Origine	Da compilare	Indica la fonte dell'azione: gap analysis NIS, vulnerabilità o remediation, incidente o lesson learned, audit interno, audit di certificazione, riesame di politiche/processi, esigenza organizzativa o tecnologica, fornitore/contratto/servizio esterno, aggiornamento normativo/perimetro/contesto.
Natura intervento	Da compilare	Tipologia dell'intervento: documentale, organizzativa, procedurale, tecnologica, contrattuale, formativa, verifica/test o remediation tecnica.
Priorità	Da compilare	Valore sintetico di priorità, definito considerando conformità, impatto organizzativo-operativo, fattibilità, scadenze e dipendenze.
Responsabile / struttura competente	Da compilare	Struttura o ruolo responsabile dell'attuazione dell'azione.
Fornitori / dipendenze	Da compilare, ove applicabile	Fornitori, contratti, servizi esternalizzati o dipendenze esterne rilevanti.
Scadenza target	Da compilare	Data obiettivo per il completamento dell'azione.
Stato	Da compilare	Stato dell'azione: proposta, validata, pianificata, in corso, bloccata, sospesa, completata, annullata, rinviata o non applicabile.
Semaforo	Automatico	Indicatore sintetico dello stato temporale dell'azione.
Evidenza di chiusura	Da compilare a chiusura	Documento, report, verbale, atto, test, configurazione o altra evidenza verificabile.
Data chiusura	Da compilare a chiusura	Data di completamento effettivo dell'azione.
Esito / decisione	Da compilare,	Esito dell'azione, decisione assunta, motivazione di rinvio, annullamento o non applicabilità.

	ove necessario	
Impegno stanziato	Da compilare, ove applicabile	Importo già stanziato o impegnato per l'attuazione dell'azione, secondo le informazioni disponibili e il livello di dettaglio adottato dall'Ente.
Budget da stanziare	Da compilare, ove applicabile	Ulteriore fabbisogno economico stimato necessario per l'attuazione o il completamento dell'azione.
Note	Da compilare, ove necessario	Ulteriori informazioni operative o gestionali, incluse eventuali indicazioni su azioni provenienti da annualità precedenti.

Il REGP_REG03 è mantenuto in formato Excel. Il foglio Registro_Azioni costituisce la fonte analitica e aggiornata delle azioni, mentre le dashboard e le viste contenute nel Registro supportano il monitoraggio e la predisposizione delle sintesi direzionali.

La tabella di cui al capitolo 8 rappresenta una fotografia dello stato delle principali azioni alla data di predisposizione o approvazione del presente Piano e non costituisce una fonte autonoma rispetto al Registro. Le successive variazioni puntuali delle azioni, delle scadenze, dello stato di avanzamento o delle evidenze sono recepite nel REGP_REG03 e non richiedono la revisione del presente Piano, salvo che comportino modifiche sostanziali delle linee di adeguamento, delle priorità complessive o dell'ambito di applicazione.

9 Sintesi delle azioni di adeguamento

Titolo azione	Descrizione sintetica / criticità	Priorità	Responsabile / struttura competente	Scadenza target
Pianificazione ed esecuzione di vulnerability assessment e penetration test	Definire il perimetro, la periodicità e le modalità di esecuzione delle attività di vulnerability assessment e, ove applicabile, penetration test sui sistemi informativi e di rete rilevanti. Documentare le attività svolte, le vulnerabilità rilevate, il relativo livello di impatto e le conseguenti azioni di trattamento.	Alta - Azione prioritaria	Settore A1911A	31/12/2026
Attuazione del programma di formazione e consapevolezza sulla sicurezza informatica	Proseguire e rendere strutturata la formazione in materia di sicurezza informatica, differenziando i contenuti per personale generale, organi di amministrazione e direttivi, personale con ruoli cyber, amministratori di sistema e personale coinvolto nella gestione degli incidenti. Mantenere evidenza di destinatari, contenuti, partecipazione ed eventuali verifiche di apprendimento.	Media - Azione rilevante ma non immediatamente bloccante	Settore A1911A	31/12/2027
Razionalizzazione e messa in sicurezza del parco applicativo	Valutare lo stato di supporto, aggiornamento, sicurezza e sostenibilità del parco applicativo e definire gli interventi di razionalizzazione necessari. La migrazione verso servizi cloud deve essere considerata per i sistemi per i quali risulti appropriata, sostenibile e coerente con i requisiti applicabili, senza assumere che il trasferimento al cloud costituisca di per sé una misura di adeguamento NIS.	Bassa - Azione migliorativa o da programmare	Settore A1911A	31/12/2026
Estensione del supporto strumentale alla gestione delle vulnerabilità	Estendere l'utilizzo di CODEMETRIC al perimetro di sistemi e applicazioni non ancora coperto, definendo il raccordo con il processo di gestione delle vulnerabilità e con il registro delle remediation.	Media - Azione rilevante ma non immediatamente bloccante	Settore A1911A	31/12/2026
Aggiornamento della gap analysis	Aggiornamento della gap analysis e consolidamento della matrice requisiti-evidenze	Bassa - Azione migliorativa o da	Settore A1911A	30/01/2027

		programmare		
Approvazione, diffusione e attuazione dell'impianto documentale di sicurezza informatica	Completare il raccordo tra politiche, piani, procedure e registri predisposti dall'Ente; verificare la copertura dei requisiti applicabili; sottoporre i documenti alle approvazioni previste; renderli disponibili alle strutture interessate e avviarne l'attuazione operativa.	Alta - Azione prioritaria	Settore A1911A	30/09/2026
Adeguamento continuativo dell'impianto documentale agli aggiornamenti normativi NIS	Monitorare la pubblicazione degli atti, delle specifiche e delle indicazioni applicative attese nell'ottobre 2026; valutarne l'impatto sull'organizzazione, sui processi e sull'impianto documentale; aggiornare i documenti interessati, la matrice requisiti-evidenze, la gap analysis e il Registro delle azioni.	Media - Azione rilevante ma non immediatamente bloccante	Settore A1911A	31/12/2026
Consolidamento degli inventari di asset, software, servizi e flussi	Integrare gli inventari esistenti assicurando la copertura di apparati fisici, dispositivi mobili, apparati di rete, stampanti, sistemi di edificio, sedi remote, software, applicazioni, servizi cloud, servizi gestiti da fornitori e flussi di rete verso l'esterno.	Media - Azione rilevante ma non immediatamente bloccante	Settore A1911A	31/12/2027
Attuazione del processo di gestione del rischio cyber negli affidamenti ICT	Approvare e rendere operativo il modello regionale per l'inserimento proporzionato dei requisiti di sicurezza negli affidamenti ICT. Definire le modalità con cui RUP e strutture committenti identificano le forniture rilevanti, selezionano i requisiti cyber, coinvolgono le funzioni competenti e conservano le evidenze.	Alta - Azione prioritaria	Settore A1911A	31/12/2026
Aggiornamento e attuazione dei piani di continuità operativa, ripristino in caso di disastro e gestione delle crisi	Completare l'aggiornamento e l'attuazione dei piani di continuità operativa, ripristino in caso di disastro e gestione delle crisi, assicurandone il raccordo con il REGP_PR01 – Procedure per la sicurezza informatica e con il REGP_REG04 – Perimetro di continuità operativa e ripristino. Consolidare per i sistemi e servizi rilevanti le priorità, i parametri di continuità e ripristino, le dipendenze e i riferimenti alla documentazione tecnica applicabile, nonché pianificare test ed esercitazioni proporzionati alla criticità dei servizi.	Alta - Azione prioritaria	Settore A1911A	31/12/2027
Estensione della cifratura dei dischi delle postazioni di lavoro portatili	Definire e attuare un piano per l'adozione della cifratura completa dei dischi dei notebook assegnati al personale regionale, prioritariamente per i dispositivi utilizzati fuori sede o sui quali sono trattati dati o informazioni dell'Ente. Il piano deve comprendere il censimento dei dispositivi, la verifica della compatibilità tecnica, l'attivazione controllata della cifratura, la gestione e custodia delle chiavi di recupero, il monitoraggio della copertura e la gestione delle eventuali eccezioni.	Media - Azione rilevante ma non immediatamente bloccante	Settore A1910A	31/12/2026
Distribuzione degli smartphone aziendali e attivazione della gestione centralizzata dei dispositivi mobili	Definire e attuare un programma per l'assegnazione progressiva di smartphone aziendali al personale regionale e per la relativa gestione centralizzata mediante una soluzione Mobile Device Management. L'intervento deve consentire il censimento e l'associazione dei dispositivi agli assegnatari, l'applicazione uniforme delle configurazioni di sicurezza, la gestione del ciclo di vita, l'installazione controllata delle applicazioni istituzionali, il blocco o la cancellazione da remoto in caso di furto o smarrimento e l'utilizzo del dispositivo gestito a supporto dell'autenticazione multifattore.	Alta - Azione prioritaria	Settore A1910A	31/10/2026
Evoluzione applicativo ARES per accesso tramite SPID / CIE	L'applicativo ARES20, attualmente fornito dal MIM e sviluppato da Soluzioni SRL, presenta per Regione Piemonte una modalità di accesso basata su credenziali deboli (username e password). E' previsto il rilascio della versione successiva (ARES30) che	Media - Azione rilevante ma non immediatamen	Settore A1501C	31/05/2027

in sostituzione di username e password	consentirà l'accesso tramite SPID / CIE.	te bloccante		

10 Allegato 1 – REGP_REG03 - Registro operativo delle azioni di adeguamento

L'Allegato 1 è costituito dal file: REGP_REG03_Registro_operativo_azioni_adeguamento_NIS.xlsx. Il file contiene il dettaglio operativo delle azioni di adeguamento e viene aggiornato secondo le modalità definite nel presente Piano.

PIANO DI FORMAZIONE IN MATERIA DI SICUREZZA INFORMATICA

Verifiche ed approvazioni

ver.	redazione		controllo ed approvazione		autorizzazione all'emissione	
	nome	data	nome	data	nome	data
v01						

Stato delle variazioni

ver.	paragrafo o pagina	descrizione della variazione
v01	Tutto il documento	Prima versione del documento

INDICE

1 FINALITÀ E RACCORDO CON LA PROGRAMMAZIONE FORMATIVA DELL'ENTE.....1

2 DESTINATARI DELLA FORMAZIONE.....2

3 AMBITI E CONTENUTI FORMATIVI.....2

3.1 FORMAZIONE PER GLI ORGANI DI AMMINISTRAZIONE E DIRETTIVI.....2

3.2 FORMAZIONE PER RUOLI SPECIALIZZATI.....3

3.3 FORMAZIONE PER TUTTO IL PERSONALE....4
4 FORMAZIONE CONTINUA E AGGIORNAMENTO....4
5 PIANIFICAZIONE, TRACCIAMENTO E VERIFICA....5
6 AGGIORNAMENTO DEL PIANO....5

1 FINALITÀ E RACCORDO CON LA PROGRAMMAZIONE FORMATIVA DELL'ENTE

Il presente Piano definisce gli indirizzi e i contenuti di riferimento per la formazione in materia di sicurezza informatica della Regione Piemonte.

Esso costituisce l'integrazione specialistica, per gli aspetti di cybersicurezza, della più ampia programmazione formativa dell'Ente e si raccorda con i processi, gli strumenti e le responsabilità adottati dalla Regione Piemonte per la rilevazione dei fabbisogni, la pianificazione, l'erogazione e la tracciatura delle attività formative.

Il Piano individua le principali categorie di destinatari, gli obiettivi formativi e gli ambiti tematici da assicurare nel tempo. La programmazione delle singole iniziative, incluse durata, calendario, modalità di erogazione e platea effettiva dei partecipanti, è definita nell'ambito della programmazione formativa vigente.

Il Piano è attuato in coerenza con il REGP_POL01 – Organizzazione per la sicurezza informatica e con il REGP_POL02 – Politiche per la sicurezza informatica.

2 DESTINATARI DELLA FORMAZIONE

Le attività formative sono differenziate in funzione del ruolo, delle responsabilità attribuite e del livello di esposizione ai rischi di sicurezza informatica.

Il Piano considera in particolare:

- gli organi di amministrazione e direttivi, per gli aspetti di governo, responsabilità e supervisione della sicurezza informatica;
- il personale che svolge ruoli specialistici, tecnici o comunque caratterizzati da specifiche responsabilità in materia di sicurezza informatica;
- tutto il personale regionale, per gli aspetti generali di consapevolezza, prevenzione e corretto comportamento nell'utilizzo dei sistemi e dei servizi digitali.

Specifici approfondimenti possono essere rivolti a ulteriori categorie di personale in relazione alle responsabilità esercitate, ai processi di competenza, ai rischi rilevati o a particolari esigenze formative.

La platea effettiva dei destinatari, le modalità di erogazione e le tempistiche delle singole iniziative sono determinate nell'ambito della programmazione formativa dell'Ente, tenendo conto dell'organizzazione vigente e delle esigenze di aggiornamento rilevate.

3 AMBITI E CONTENUTI FORMATIVI

I contenuti delle iniziative formative sono definiti e aggiornati in funzione dei destinatari e del relativo fabbisogno. I programmi dei singoli corsi possono approfondire o integrare gli argomenti di seguito indicati in relazione all'evoluzione normativa, organizzativa, tecnologica e delle minacce.

3.1 FORMAZIONE PER GLI ORGANI DI AMMINISTRAZIONE E DIRETTIVI

La formazione è finalizzata a fornire gli elementi necessari alla comprensione del rischio cyber e all'esercizio consapevole delle responsabilità di governo, indirizzo e supervisione previste dall'assetto organizzativo e dalla disciplina applicabile.

Gli ambiti formativi comprendono almeno:

- quadro generale delle minacce e dei rischi di sicurezza informatica rilevanti per una pubblica amministrazione;
- quadro normativo NIS e responsabilità degli organi di amministrazione e direttivi;
- organizzazione per la sicurezza informatica della Regione Piemonte;
- gestione e trattamento del rischio cyber;
- principali misure organizzative e tecniche di sicurezza;
- gestione degli incidenti e relativi obblighi di comunicazione e notifica;
- continuità operativa, ripristino in caso di disastro e gestione delle crisi;
- governo e monitoraggio dell'attuazione delle misure di sicurezza.

3.2 FORMAZIONE PER RUOLI SPECIALIZZATI

La formazione dedicata al personale con compiti specialistici o tecnici è definita in relazione alle attività effettivamente svolte e alle responsabilità attribuite.

Gli ambiti formativi possono comprendere, secondo applicabilità:

- quadro normativo e organizzativo di riferimento;
- configurazione e funzionamento sicuri dei sistemi informativi e di rete;
- minacce informatiche note e principali modalità di attacco;
- politiche, procedure e istruzioni di sicurezza applicabili;
- gestione degli incidenti e comportamento da adottare in presenza di eventi rilevanti per la sicurezza;
- gestione delle vulnerabilità e degli aggiornamenti;
- gestione degli accessi e dei privilegi;
- logging e monitoraggio;
- continuità operativa e ripristino in caso di disastro;
- ulteriori contenuti specialistici coerenti con le attività e i sistemi gestiti.

3.3 FORMAZIONE PER TUTTO IL PERSONALE

La formazione rivolta al personale regionale è finalizzata a sviluppare un livello adeguato di consapevolezza dei rischi di sicurezza informatica e a favorire comportamenti coerenti con le politiche e le procedure adottate dall'Ente.

Gli ambiti formativi comprendono almeno:

- principi essenziali di sicurezza informatica e responsabilità individuali nell'utilizzo degli strumenti dell'Ente;
- corretto utilizzo di credenziali, sistemi di autenticazione e strumenti di lavoro;
- riconoscimento di phishing, smishing, social engineering e altre comunicazioni sospette;
- utilizzo sicuro della posta elettronica, dei dispositivi, dei servizi digitali e degli strumenti di collaborazione;
- protezione delle informazioni trattate;
- principali rischi derivanti dall'utilizzo improprio o non autorizzato degli strumenti digitali;
- modalità di segnalazione di anomalie, eventi sospetti e incidenti di sicurezza;
- comportamenti da adottare in caso di sospetta compromissione, perdita di dispositivi o credenziali.

4 FORMAZIONE CONTINUA E AGGIORNAMENTO

La formazione in materia di sicurezza informatica non è limitata alla partecipazione a singoli corsi, ma costituisce un processo continuativo di aggiornamento e sensibilizzazione.

Le esigenze formative sono riesaminate nel tempo tenendo conto, in particolare:

- dell'evoluzione delle minacce e delle tecniche di attacco;
- delle modifiche normative e delle indicazioni delle autorità competenti;
- dell'evoluzione dell'organizzazione, dei servizi e delle tecnologie utilizzate;
- delle modifiche alle politiche, ai piani e alle procedure di sicurezza informatica;
- degli incidenti, degli eventi rilevanti e delle relative lesson learned;
- degli esiti delle attività di valutazione del rischio, verifica e audit;
- delle specifiche esigenze connesse ai ruoli e alle responsabilità esercitate.

L'aggiornamento può essere realizzato mediante corsi periodici, moduli di richiamo o approfondimento, iniziative di sensibilizzazione, comunicazioni tematiche, esercitazioni e ulteriori modalità formative ritenute appropriate.

Le iniziative sono integrate, per quanto possibile, nella programmazione formativa ordinaria della Regione Piemonte.

5 PIANIFICAZIONE, TRACCIAMENTO E VERIFICA

La pianificazione delle iniziative formative in materia di sicurezza informatica è integrata negli strumenti e nei processi utilizzati dalla Regione Piemonte per la programmazione e la gestione della formazione del personale.

Per ciascuna iniziativa formativa sono mantenute, attraverso i sistemi e le modalità adottati dall'Ente, evidenze adeguate a documentare almeno i destinatari o i partecipanti, i contenuti effettivamente erogati e, ove previste, le verifiche dell'acquisizione dei contenuti.

I programmi di dettaglio dei singoli corsi, i calendari, le modalità di erogazione, i registri di partecipazione, le attestazioni e gli esiti delle eventuali verifiche sono mantenuti nell'ambito della documentazione e dei sistemi ordinari di gestione della formazione della Regione Piemonte e non sono duplicati nel presente Piano.

Il presente Piano definisce pertanto gli obiettivi e gli ambiti formativi di riferimento, mentre la programmazione e la documentazione delle singole iniziative ne costituiscono attuazione operativa.

Le modalità di verifica dell'apprendimento sono definite in funzione della tipologia e degli obiettivi dell'attività formativa e possono comprendere, ove opportuno, test, questionari, attestazioni di completamento, esercitazioni o altre forme di riscontro.

6 AGGIORNAMENTO DEL PIANO

Il presente Piano è riesaminato e, ove necessario, aggiornato in relazione all'evoluzione del quadro normativo e organizzativo, dei rischi, delle minacce, delle tecnologie e dei fabbisogni formativi rilevati.

L'aggiornamento della programmazione annuale, del calendario, dei partecipanti, delle modalità di erogazione o dei singoli programmi didattici non comporta di per sé la revisione del presente Piano, qualora non ne modifichi gli obiettivi, i destinatari o l'impostazione generale.

PIANO DI CONTINUITÀ OPERATIVA

VERIFICHE ED APPROVAZIONI

VER.	REDAZIONE		CONTROLLO ED APPROVAZIONE		AUTORIZZAZIONE ALL'EMISSIONE	
	NOME	DATA	NOME	DATA	NOME	DATA

STATO DELLE VARIAZIONI

ver.	paragrafo o pagina	descrizione della variazione
	Tutto il documento	Versione iniziale del documento

SOMMARIO

INDICE DELLE ABBREVIAZIONI 3
1 PREMESSA 4
1.1 Contesto 4
1.2 Relazione con il sistema documentale 4
1.3 Perimetro del Piano 5
1.4 Relazione con ID.IM-04 5
2 FINALITÀ E AMBITO DI APPLICAZIONE 5
2.1 Finalità 5
2.2 Ambito di applicazione 6
2.3 Obiettivi del Piano 6
2.4 Principi di Continuità Operativa 6
3 MODELLO DI CONTINUITÀ OPERATIVA 7
3.1 Framework di continuità 7
3.2 Parametri di continuità 7
4 RUOLI E RESPONSABILITÀ 8
4.1 Raccordo con la matrice RACI 9
5 CONTATTI PRINCIPALI 9
5.1 Gestione della reperibilità 10
6 COMUNICAZIONE 10
6.1 Obiettivi 10
6.2 Livelli di comunicazione 11
7 ATTIVAZIONE E DISATTIVAZIONE DEL PIANO 11
7.1 Livelli di attivazione 12
7.2 Processo di attivazione 12
8 STRATEGIE DI CONTINUITÀ 13
9 DIPENDENZE CRITICHE 14
10 TEST ED ESERCITAZIONI 14
10.1 Programma annuale 16
10.2 Formazione 16
11 MANUTENZIONE DEL PIANO 16
11.1 Riesame straordinario 16
11.2 Miglioramento continuo 17
12 KPI DELLA CONTINUITÀ OPERATIVA 17
13 RACCORDI OPERATIVI E FONTI INFORMATIVE 17
13.1 Presidi condivisi 18

INDICE DELLE ABBREVIAZIONI

ACN *Agenzia per la Cybersicurezza Nazionale*
BCP *Business Continuity Plan*
BIA *Business Impact Analysis*
CISO *Chief Information Security Officer*
CIO *Chief Information Officer*
CSIRT *Computer Security Incident Response Team*
DR *Disaster Recovery*
ICT *Information and Communication Technology*
ID.IM *Identify - Incident Management*
IRT *Incident Response Team*
NIS2 *Direttiva (UE) 2022/2555 sulla cybersicurezza*
RPO *Recovery Point Objective*
RTO *Recovery Time Objective*
MTPD *Maximum Tolerable Period of Disruption*
SIEM *Security Information and Event Management*
SLA *Service Level Agreement*
SOC *Security Operations Center*

1 PREMESSA

Il presente Piano di Continuità Operativa (PCO) definisce il quadro strategico e organizzativo adottato dalla Regione Piemonte per garantire la continuità dei sistemi informativi e di rete rilevanti.

Il Piano è redatto in conformità alla Direttiva (UE) 2022/2555 (NIS2), al D.lgs. 138/2024 e alle disposizioni dell'Agenzia per la Cybersicurezza Nazionale (ACN – ID.IM-04).

Il PCO costituisce parte integrante del sistema di gestione della sicurezza e resilienza della Regione Piemonte e si integra con:

- il Piano di Gestione delle Crisi, che disciplina la governance degli eventi critici;
- il Piano di Ripristino in caso di Disastro (DRP), che disciplina le procedure tecniche di ripristino.

1.1 Contesto

La continuità operativa rappresenta una componente fondamentale del sistema di gestione della sicurezza e della resilienza della Regione Piemonte.

L'evoluzione delle minacce cyber, la crescente dipendenza dai sistemi informativi e la rilevanza dei servizi digitali erogati rendono necessario adottare un modello strutturato di Business Continuity in grado di garantire la continuità delle funzioni essenziali anche in presenza di eventi avversi.

La Regione Piemonte eroga e supporta un insieme articolato di servizi digitali rivolti ai cittadini, alle imprese, agli enti territoriali, al sistema sanitario e alle strutture dell'Amministrazione regionale. La continuità di tali servizi rappresenta un elemento essenziale per il corretto svolgimento delle funzioni istituzionali e per il mantenimento dei livelli di servizio attesi dagli stakeholder.

Il presente Piano definisce il quadro di riferimento organizzativo e strategico adottato dalla Regione Piemonte per prevenire, gestire e mitigare gli impatti derivanti da eventi che possano compromettere la disponibilità dei servizi informativi e di rete rilevanti come richiesto dalla NIS2 e specificato in premessa.

1.2 Relazione con il sistema documentale

Il Piano si inserisce nell'impianto documentale di sicurezza informatica della Regione Piemonte e si raccorda, per i rispettivi ambiti, con:

- il REGP_POL01 – Organizzazione per la sicurezza informatica, per ruoli, responsabilità e raccordi organizzativi;
- il REGP_POL02 – Politiche per la sicurezza informatica, per i principi generali di continuità, ripristino e resilienza;
- il Piano di gestione degli incidenti di sicurezza informatica, per la gestione degli eventi e degli incidenti;
- il Piano di gestione delle crisi, per i meccanismi straordinari di coordinamento e decisione;
- il Piano di ripristino in caso di disastro, per il recupero delle componenti tecnologiche, dei sistemi e dei dati;

- il REGP_PR01 – Procedure per la sicurezza informatica, per le modalità operative comuni di attuazione;
- il REGP_REG04 – Perimetro di continuità operativa e ripristino, nel quale sono mantenute le informazioni dinamiche condivise necessarie all'attuazione del presente Piano e del Piano di ripristino in caso di disastro.

Le istruzioni e i runbook tecnici riferiti a specifici sistemi o servizi sono mantenuti dalle strutture competenti, da CSI Piemonte o dagli ulteriori soggetti gestori e sono richiamati, ove necessario, senza duplicarne il contenuto nel presente Piano.

1.3 Perimetro del Piano

Il presente Piano si applica almeno ai sistemi informativi e di rete rilevanti individuati dalla Regione Piemonte. La definizione e il riesame del perimetro tengono conto delle informazioni disponibili sulla criticità dei servizi e delle funzioni istituzionali supportate, degli esiti della Business Impact Analysis, delle valutazioni del rischio e delle principali dipendenze organizzative, tecnologiche ed esterne.
L'elenco vigente dei sistemi e dei servizi ricompresi nel perimetro, unitamente ai relativi parametri di continuità e ripristino, è mantenuto nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

1.4 Relazione con ID.IM-04

Il presente Piano assicura la copertura dei contenuti previsti dalla misura ID.IM-04 per il Piano di continuità operativa.

Riferimento	Contenuto	Copertura
ID.IM-04, punto 1, lett. a)	Finalità, esigenze di continuità e ambito di applicazione	Premessa; §§1.3, 2.1, 2.2, 3
ID.IM-04, punto 1, lett. b)	Ruoli e responsabilità	Cap. 4 e REGP_POL01
ID.IM-04, punto 1, lett. c)	Contatti principali e canali di comunicazione interni ed esterni	Capp. 5 e 6 e fonti operative richiamate
ID.IM-04, punto 1, lett. d)	Condizioni di attivazione e disattivazione	Cap. 7
ID.IM-04, punto 1, lett. e)	Risorse necessarie, inclusi backup e ridondanze	Cap. 8 e documentazione tecnica applicabile
ID.IM-04, punto 4	Approvazione	Frontespizio e processo di approvazione dell'Ente
ID.IM-04, punto 5	Riesame periodico e straordinario	Cap. 12

Le dipendenze, i test, le evidenze e le attività di miglioramento costituiscono elementi di supporto all'attuazione e al mantenimento del Piano e non ulteriori lettere del punto 1 della misura.

2 FINALITÀ E AMBITO DI APPLICAZIONE

2.1 Finalità

Ai fini del presente Piano, per i sistemi informativi e di rete rilevanti si intendono i sistemi e i servizi digitali il cui malfunzionamento, indisponibilità o compromissione potrebbe determinare impatti significativi sulla

continuità delle funzioni istituzionali o sull'erogazione dei servizi individuati dalla Regione nell'ambito dei processi di classificazione previsti dalla normativa NIS2.

Il PCO ha la finalità di:

- assicurare la continuità dei servizi supportati dai sistemi informativi e di rete rilevanti;
- definire i criteri per l'attivazione e la disattivazione delle misure di continuità;
- stabilire le priorità e le strategie generali di continuità in coerenza con le esigenze individuate dalla Business Impact Analysis e con gli esiti delle valutazioni del rischio;
- assicurare il raccordo con il Piano di gestione degli incidenti, il Piano di gestione delle crisi e il Piano di ripristino in caso di disastro.

Il Piano non disciplina le modalità di governo della crisi né le procedure tecniche di ripristino, disciplinate dai rispettivi piani e dalla documentazione operativa applicabile.
Il perimetro vigente dei sistemi e dei servizi interessati è mantenuto nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

2.2 Ambito di applicazione

Il Piano si applica ai sistemi informativi e di rete ricompresi nel perimetro di continuità operativa della Regione Piemonte e alle funzioni e ai servizi da essi supportati.

Sono coinvolte, secondo le rispettive competenze, le strutture regionali titolari o interessate dai servizi, nonché CSI Piemonte, gli ulteriori soggetti in house, i fornitori e le terze parti che concorrono alla loro erogazione. Per i soggetti esterni, compiti, livelli di servizio, contatti ed eventuali obblighi in materia di continuità e ripristino restano disciplinati dai relativi contratti, convenzioni, accordi di servizio e dalle ulteriori fonti operative adottate dall'Ente.

2.3 Obiettivi del Piano

ll Piano si pone i seguenti obiettivi:

- garantire la continuità dei servizi rilevanti;
- ridurre il rischio di indisponibilità prolungata;
- minimizzare gli impatti su cittadini, imprese ed enti;
- assicurare adeguati livelli di resilienza operativa;
- supportare il processo decisionale nelle situazioni emergenziali;
- garantire il coordinamento con il Piano di Gestione delle Crisi e con il Piano di Disaster Recovery.

2.4 Principi di Continuità Operativa

Le misure di continuità operativa sono definite secondo criteri di rischio e proporzionalità, tenendo conto della criticità dei servizi, degli impatti dell'indisponibilità, delle dipendenze e delle capacità di recupero disponibili.

Il processo di continuità opera in coordinamento con la gestione degli incidenti, il ripristino in caso di disastro e la gestione delle crisi, secondo i principi definiti nel REGP_POL02 – Politiche per la sicurezza informatica. L'efficacia delle misure è verificata attraverso attività di test, esercitazione e riesame proporzionate alla criticità e ai rischi dei servizi interessati.

3 MODELLO DI CONTINUITÀ OPERATIVA

3.1 Framework di continuità

La continuità operativa della Regione Piemonte è basata su un modello integrato che collega le attività di classificazione, analisi, gestione del rischio, pianificazione e miglioramento continuo. Il framework assicura la coerenza tra i processi di individuazione dei servizi rilevanti, la definizione delle strategie di continuità e le attività di risposta e ripristino.

Fase	Elemento del modello	Finalità
1	Classificazione dei servizi	Classificazione dei servizi secondo i criteri adottati dalla Regione Piemonte
↓		Individuazione del livello di criticità
2	Individuazione dei servizi rilevanti	Identificazione dei servizi soggetti alle misure di continuità operativa
↓		Definizione del perimetro di analisi
3	Business Impact Analysis (BIA)	Analisi degli impatti derivanti dall'indisponibilità dei servizi
↓		Determinazione di RTO, RPO e MTPD
4	Risk Assessment	Valutazione dei rischi che possono compromettere la continuità operativa
↓		definizione delle priorità di trattamento
5	Strategie di Continuità Operativa	Individuazione delle misure organizzative, tecnologiche e logistiche di continuità
↓		Integrazione con i piani specialistici
6	Piano di Gestione delle Crisi	Gestione della governance e dei processi decisionali durante eventi critici
7	Piano di Disaster Recovery	Ripristino tecnico dei sistemi informativi e di rete
↓		Verifica dell'efficacia delle misure
8	Test ed esercitazioni	Validazione periodica delle strategie e delle procedure
↓		Raccolta evidenze e lesson learned
9	**Miglioramento continuo**	

Le attività di classificazione dei servizi, identificazione dei servizi rilevanti, Business Impact Analysis e Risk Assessment sono soggette a riesame periodico e costituiscono input per l'aggiornamento delle strategie di continuità operativa, del Piano di Gestione delle Crisi e del Piano di Disaster Recovery.

3.2 Parametri di continuità

I parametri di continuità operativa rappresentano il riferimento utilizzato dalla Regione Piemonte per qualificare le esigenze di resilienza dei servizi informativi e di rete rilevanti, definire le priorità di intervento e orientare le strategie di continuità e di ripristino. Tali parametri sono determinati nell'ambito delle attività

di classificazione dei servizi, Business Impact Analysis (BIA) e Risk Assessment e sono riesaminati periodicamente in coerenza con l'evoluzione del perimetro dei servizi, delle dipendenze critiche e dei livelli di rischio.
In particolare, i parametri consentono di stabilire il livello minimo di servizio da preservare o ripristinare, i tempi massimi accettabili di indisponibilità, la perdita di dati sostenibile e le priorità di recupero in caso di evento critico. Essi costituiscono quindi un input essenziale per la definizione delle misure organizzative, tecnologiche, logistiche e contrattuali previste dal presente Piano, dal Piano di Gestione delle Crisi e dal Piano di Disaster Recovery.

Recovery Time Objective (RTO)
Il Recovery Time Objective rappresenta il tempo massimo entro il quale un servizio deve essere ripristinato a seguito di un'interruzione, al fine di evitare impatti non accettabili sulle funzioni istituzionali e sui servizi erogati. Il valore di RTO orienta la scelta delle strategie di recupero, delle soluzioni di ridondanza e delle procedure operative di ripristino.

Recovery Point Objective (RPO)
Il Recovery Point Objective esprime la massima perdita di dati ritenuta accettabile in caso di indisponibilità o compromissione del servizio. Il parametro è utilizzato per definire i requisiti di backup, replica, protezione, conservazione e recupero delle informazioni.

Maximum Tolerable Period of Disruption (MTPD)
Il Maximum Tolerable Period of Disruption indica il periodo massimo di indisponibilità oltre il quale gli impatti sull'organizzazione, sugli utenti o sulle funzioni istituzionali diventano non accettabili. Il valore di MTPD costituisce il limite superiore entro cui devono essere attuate le misure di continuità e ripristino.

Livello di criticità del servizio
Il livello di criticità esprime la rilevanza del servizio rispetto alle funzioni istituzionali della Regione Piemonte e agli impatti derivanti dalla sua indisponibilità. Tale parametro consente di stabilire le priorità di intervento, allocare le risorse disponibili e individuare i servizi da sottoporre a misure più stringenti di continuità operativa.

Dipendenze critiche
Le dipendenze critiche identificano le risorse, le infrastrutture, le componenti tecnologiche, le competenze e i soggetti esterni necessari all'erogazione del servizio. La loro analisi permette di valutare eventuali punti di fragilità, definire misure di mitigazione e predisporre soluzioni alternative o procedure di escalation.

I valori applicabili ai singoli sistemi e servizi, unitamente alle principali dipendenze rilevanti ai fini della continuità e del ripristino, sono mantenuti nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

4 RUOLI E RESPONSABILITÀ

L'assetto generale dei ruoli, delle responsabilità e dei raccordi organizzativi in materia di cybersicurezza è definito nel documento **REGP_POL01 - Organizzazione per la Sicurezza Informatica**, che costituisce il riferimento organizzativo unitario dell'Ente. Il presente Piano non ridefinisce tale assetto e individua esclusivamente i raccordi funzionali necessari all'attuazione delle misure di continuità operativa.
Il Piano è approvato dagli organi di amministrazione e direttivi competenti secondo quanto previsto dalla normativa applicabile, dagli atti organizzativi dell'Ente e dal REGP_POL01.

Per i profili specificamente attinenti alla cybersicurezza, il presidio tecnico-organizzativo della continuità operativa è assicurato dal **Settore A1911A - Sistema informativo regionale**, in raccordo con il **Settore A1910A - Servizi infrastrutturali e tecnologici** e con le altre strutture regionali competenti in relazione ai servizi e ai processi interessati.
Le strutture regionali competenti concorrono all'attuazione delle misure di continuità per gli ambiti di rispettiva competenza. I fornitori, i soggetti terzi e gli eventuali soggetti in house assicurano il supporto tecnico-operativo e l'attuazione delle misure loro attribuite nei limiti previsti dai relativi contratti, convenzioni, disciplinari o accordi di servizio.
Il **Punto di contatto NIS2** e il **Referente CSIRT** intervengono, ove applicabile, nell'ambito delle rispettive competenze per gli adempimenti, le comunicazioni e le notifiche previsti dalla disciplina NIS, secondo quanto definito nel REGP_POL01 e nel Piano di Gestione degli Incidenti.
Qualora l'evento determini l'attivazione della gestione della crisi, si applicano i ruoli, le responsabilità e i meccanismi decisionali previsti dal Piano di Gestione delle Crisi.

4.1 Raccordo con la matrice RACI

Al fine di evitare duplicazioni o attribuzioni non coerenti con l'assetto organizzativo dell'Ente, il presente Piano non introduce una matrice RACI autonoma dei ruoli di cybersicurezza. Per le responsabilità organizzative si applica la matrice RACI definita nel **REGP_POL01 - Organizzazione per la Sicurezza Informatica**.

Le responsabilità operative specifiche relative all'attivazione, all'esecuzione e alla disattivazione delle misure di continuità sono esercitate, in relazione al servizio e all'evento interessato, dalle strutture competenti e dai fornitori secondo quanto previsto dal presente Piano, dagli atti organizzativi dell'Ente e dai relativi contratti o accordi di servizio.

5 CONTATTI PRINCIPALI

La disponibilità di riferimenti nominativi aggiornati, verificabili e immediatamente contattabili costituisce un requisito essenziale per l'efficace gestione della continuità operativa. In situazioni di emergenza o di interruzione dei servizi, la tempestività delle comunicazioni e delle decisioni rappresenta un fattore determinante per ridurre gli impatti e garantire il coordinamento delle attività di risposta.

Per tale motivo la Regione Piemonte identifica preventivamente le risorse che, a diverso titolo, possono essere coinvolte nelle attività di continuità operativa, gestione degli incidenti, gestione delle crisi e ripristino dei servizi, assicurando la disponibilità di informazioni di contatto costantemente aggiornate.

I riferimenti comprendono personale interno, responsabili di servizio, strutture di supporto, fornitori rilevanti e soggetti esterni che possono essere coinvolti nelle attività di risposta agli eventi.

A garanzia dell'aggiornamento e dell'unicità delle informazioni, i nominativi e i recapiti relativi ai ruoli di sicurezza informatica sono mantenuti nella fonte ufficiale individuata dall'Ente nell'ambito del REGP_POL01.
I riferimenti operativi relativi alle strutture, ai servizi e ai fornitori coinvolti nelle attività di continuità e ripristino sono mantenuti nelle fonti organizzative, contrattuali e operative vigenti e, ove pertinente, richiamati nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

5.1 Gestione della reperibilità

La reperibilità delle risorse critiche è garantita mediante:

- contatti primari;
- contatti secondari;
- meccanismi di escalation;
- copertura in caso di assenza prolungata.

Le modalità operative di reperibilità, i turni, le modalità di contatto e le procedure di escalation sono disciplinate, ove applicabili, nel REGP_PR01 – Procedure per la sicurezza informatica, nei documenti operativi relativi ai singoli servizi e nei contratti o accordi di servizio applicabili.

6 COMUNICAZIONE

Le attività di comunicazione previste dal presente Piano sono coordinate con quanto stabilito nel Piano di Gestione degli Incidenti, nel Piano di Gestione delle Crisi e nel documento REGP_PR01 - Procedure per la Sicurezza Informatica, al fine di garantire coerenza dei flussi informativi e delle responsabilità.

6.1 Obiettivi

Le comunicazioni previste dal presente Piano hanno lo scopo di garantire che le informazioni necessarie alla gestione degli eventi che impattano la continuità operativa siano trasmesse ai soggetti competenti in modo tempestivo, accurato, coerente e tracciabile.

In particolare, il processo di comunicazione è finalizzato a:

- assicurare la tempestiva attivazione delle strutture organizzative e dei soggetti coinvolti nelle attività di continuità operativa;
- garantire la condivisione di informazioni corrette, aggiornate e coerenti sullo stato dell'evento, sugli impatti rilevati e sulle azioni intraprese;
- supportare il coordinamento delle attività operative, tecniche e decisionali tra le strutture interne e le terze parti coinvolte;
- favorire l'adozione tempestiva delle decisioni da parte dei soggetti responsabili della gestione dell'evento;
- assicurare il rispetto degli obblighi di comunicazione e notifica previsti dalla normativa applicabile e dalle procedure interne;
- garantire la tracciabilità delle comunicazioni effettuate e delle informazioni condivise durante tutte le fasi di gestione dell'evento;
- contribuire alla riduzione dei tempi di risposta e alla mitigazione degli impatti sui servizi rilevanti.

Le modalità operative, i canali di comunicazione, i soggetti coinvolti, i modelli di comunicazione e i flussi informativi sono disciplinati nei documenti richiamati nel presente capitolo e nel REGP_PR01 – Procedure per la sicurezza informatica.

6.2 Livelli di comunicazione

Livello	Destinatari	Obiettivo	Documento di riferimento
Operativo	Personale ICT, IRT, fornitori rilevanti	Gestione attività di continuità	Piano di gestione degli incidenti di sicurezza informatica
Direzionale	Organi amministrativi e direttivi di vertice	Supporto decisionale	Piano di gestione delle crisi
Istituzionale	ACN, CSIRT Italia, autorità competenti	Obblighi normativi e notifiche	REGP_PR01 – Procedure per la sicurezza informatica

I processi di comunicazione e i relativi flussi informativi sono disciplinati, per quanto di rispettiva competenza, dal REGP_POL01, dal Piano di Gestione degli Incidenti, dal Piano di Gestione delle Crisi e dalle Procedure per la Sicurezza Informatica, cui il presente Piano rinvia per gli aspetti operativi.

7 ATTIVAZIONE E DISATTIVAZIONE DEL PIANO

L'attivazione del Piano di Continuità Operativa avviene sulla base di una valutazione strutturata dell'evento effettuata dalle strutture tecniche e organizzative competenti per il servizio interessato, con il coordinamento tecnico-organizzativo del Settore A1911A - Sistema informativo regionale e, per i profili infrastrutturali e tecnologici, in raccordo con il Settore A1910A - Servizi infrastrutturali e tecnologici. L'attivazione è disposta secondo le competenze organizzative vigenti dell'Ente, tenendo conto delle risultanze della Business Impact Analysis, della classificazione del servizio interessato e degli impatti attesi sull'operatività dell'Ente.

La valutazione considera in particolare:

- la criticità del servizio coinvolto;
- la durata stimata dell'interruzione;
- il numero di utenti o strutture interessate;
- l'impatto sulle funzioni istituzionali;
- la disponibilità di soluzioni alternative;
- la necessità di coinvolgere soggetti esterni o attivare escalation direzionali.

In funzione degli esiti della valutazione l'evento viene classificato secondo i livelli di attivazione previsti dal presente Piano.

Il PCO è attivato in caso di eventi che compromettono o possono compromettere la continuità dei sistemi informativi e di rete rilevanti o dei servizi rilevanti individuati nell'ambito dei processi di classificazione, Business impact Analysis e Risk Assessment. La classificazione dell'evento è basata su:

- impatto;
- estensione;
- durata attesa;
- numero servizi coinvolti;
- necessità di escalation.

Gli scenari oggetto del Piano sono:

- indisponibilità piattaforme digitali regionali;

- indisponibilità connettività;
- indisponibilità data center;
- indisponibilità fornitori rilevanti;
- eventi cyber
- indisponibilità sedi.

L'attivazione:

- è proposta dalle strutture competenti in relazione al servizio e all'evento interessato ed è disposta secondo le competenze organizzative vigenti dell'Ente, in coerenza con il REGP_POL01;
- può avvenire anche in via preventiva in presenza di rischi significativi.

L'attivazione del PCO:

- non coincide automaticamente con la dichiarazione dello stato di crisi;
- è distinta dalla gestione della crisi, disciplinata dal Piano di Gestione delle Crisi.

L'eventuale attivazione della gestione della crisi avviene secondo i criteri, i ruoli e le modalità definiti nel Piano di gestione delle crisi.
La disattivazione del Piano avviene al ripristino delle condizioni operative minime accettabili.

7.1 Livelli di attivazione

La classificazione dell'evento è effettuata mediante una valutazione congiunta della criticità del servizio coinvolto, dell'impatto atteso, dell'estensione dell'interruzione, della durata prevista e della necessità di escalation verso livelli superiori di governance. Sulla base di tali elementi l'evento viene associato ad uno dei livelli di attivazione descritti nella tabella seguente.

Livello	Descrizione	Effetto	Esempio
0	Incidente	Gestione mediate processi ordinari di Incident Management	Malfunzionamento di un singolo servizio
1	Emergenza	Attivazione delle misure di continuità previste nel PCO	Indisponibilità contemporanea di più servizi
2	Grave interruzione	Coinvolgimento degli Organi amministrativi e direttivi di vertice e monitoraggio rafforzato	Indisponibilità prolungata di un servizio rilevante con superamento dell'RTO definito o coinvolgimento di dipendenze critiche.
3	Evento con possibile rilevanza di crisi	Valutazione dell'attivazione del Piano di gestione delle crisi secondo i criteri in esso definiti	Evento che interessa contemporaneamente più servizi rilevanti o infrastrutture condivise, con necessità di attivazione della governance di crisi.

7.2 Processo di attivazione

Fase	Processo di attivazione
1	Evento
↓	*rilevazione di un'anomalia o di una condizione che può impattare la continuità*
2	Valutazione

↓	*analisi degli impatti, dei livelli di servizio e delle condizioni di attivazione*
3	Attivazione PCO
↓	*avvio delle misure di continuità e coordinamento con i ruoli competenti*
4	Monitoraggio
↓	*verifica dell'efficacia delle misure adottate e dello stato di ripristino*
5	**Disattivazione**

8 STRATEGIE DI CONTINUITÀ

Le strategie di continuità operativa della Regione Piemonte sono definite sulla base dei risultati della Business Impact Analysis (BIA), delle valutazioni di rischio effettuate dall'Ente e della classificazione dei servizi rilevanti. Esse hanno l'obiettivo di garantire il mantenimento o il rapido ripristino delle funzioni istituzionali e dei servizi digitali in caso di eventi che possano comprometterne la disponibilità.

Le strategie adottate considerano congiuntamente gli aspetti organizzativi, logistici, tecnologici e contrattuali che concorrono all'erogazione dei servizi e sono orientate a ridurre la probabilità di interruzioni prolungate e gli impatti su cittadini, imprese, enti territoriali e strutture dell'Amministrazione regionale.

La continuità operativa viene perseguita attraverso i seguenti ambiti strategici.

Ambito	Obiettivo	Principali misure
Personale	Garantire la disponibilità delle competenze necessarie alla gestione dei servizi e degli eventi emergenziali	sostituzione ruoli chiave, piani di reperibilità, lavoro agile, trasferimento competenze
Sedi e luoghi di lavoro	Assicurare la continuità delle attività anche in caso di indisponibilità delle sedi ordinarie	sedi alternative, accesso remoto sicuro, strumenti di collaborazione e comunicazione
Sistemi informativi	Garantire la disponibilità dei sistemi e delle piattaforme necessarie all'erogazione dei servizi	ridondanza delle componenti, soluzioni ad alta affidabilità, monitoraggio continuo
Dati e informazioni	Garantire disponibilità e integrità e recuperabilità delle informazioni	backup, replica, conservazione e procedure di ripristino
Fornitori rilevanti	Garantire il supporto delle terze parti necessarie all'erogazione dei servizi	gestione degli SLA, procedure di escalation, verifiche contrattuali e monitoraggio delle prestazioni

Le strategie sopra riportate costituiscono il quadro generale di riferimento per la continuità operativa della Regione Piemonte e comprendono, in relazione alle esigenze dei singoli servizi, le risorse umane, organizzative, logistiche, tecnologiche e contrattuali necessarie, incluse le misure di backup e ridondanza applicabili. Il dettaglio delle strategie e delle principali dipendenze riferite ai singoli sistemi e servizi è mantenuto nel REGP_REG04 – Perimetro di continuità operativa e ripristino; le modalità operative sono disciplinate nel REGP_PR01 – Procedure per la sicurezza informatica e, per gli aspetti tecnici specifici, nella documentazione mantenuta dalle strutture competenti e dai soggetti gestori.

9 DIPENDENZE CRITICHE

La capacità della Regione Piemonte di garantire la continuità dei servizi dipende dalla disponibilità di risorse, infrastrutture e soggetti che, a diverso titolo, contribuiscono all'erogazione dei servizi digitali e al funzionamento dei processi istituzionali.

L'identificazione preventiva delle dipendenze critiche consente di valutare gli impatti derivanti dalla loro indisponibilità, definire adeguate misure di mitigazione e predisporre strategie alternative di continuità operativa.

Le dipendenze critiche sono identificate e riesaminate nell'ambito delle attività di Business Impact Analysis e Risk Assessment e sono oggetto di aggiornamento periodico in coerenza con l'evoluzione organizzativa e tecnologica dell'Ente.

Le principali categorie di dipendenze considerate sono riportate nella tabella seguente.

Categoria	Descrizione	Esempi
Dipendenze tecnologiche	Componenti infrastrutturali e tecnologiche necessarie per il funzionamento dei servizi	Data Center, servizi cloud, connettività, reti dati, sistemi IAM, piattaforme condivise
Dipendenze organizzative	Strutture, competenze e processi necessari al funzionamento dei servizi	Personale specialistico, responsabili di servizio, funzioni direzionali e di coordinamento
Dipendenze esterne	Risorse e servizi forniti da soggetti terzi	Fornitori ICT, servizi di telecomunicazione, utilities energetiche, conservatori, provider PEC, identity provider

Per ciascuna dipendenza critica sono individuate, ove applicabili, specifiche misure di mitigazione, procedure di escalation e modalità di attivazione di soluzioni alternative. Il dettaglio delle dipendenze riferite ai singoli sistemi e servizi è mantenuto nel REGP_REG04 – Perimetro di continuità operativa e ripristino e utilizzato, per quanto pertinente, anche dal Piano di ripristino in caso di disastro.

Le dipendenze esterne sono inoltre monitorate nell'ambito dei processi di gestione dei fornitori rilevanti e della supply chain, in conformità alle disposizioni normative in materia di cybersicurezza e resilienza operativa.

10 TEST ED ESERCITAZIONI

Le attività di test e di esercitazione rappresentano uno degli elementi fondamentali del sistema di continuità operativa della Regione Piemonte e consentono di verificare periodicamente l'efficacia delle strategie adottate, il livello di preparazione delle strutture coinvolte e l'idoneità delle procedure previste dal Piano.

I test hanno inoltre lo scopo di individuare eventuali criticità, raccogliere evidenze oggettive e attivare processi di miglioramento continuo basati sulle esperienze maturate durante le attività di verifica.
In funzione degli obiettivi perseguiti possono essere utilizzate diverse tipologie di test.

Walkthrough o test documentale

Consiste nell'analisi strutturata del Piano e della documentazione correlata da parte dei soggetti coinvolti.
L'obiettivo è verificare:

- completezza della documentazione;
- correttezza delle informazioni riportate;
- aggiornamento di ruoli, responsabilità e contatti;
- coerenza con gli altri documenti del sistema di gestione.

Tabletop Exercise

È una simulazione basata sulla discussione guidata di uno scenario ipotetico.
I partecipanti analizzano gli impatti dell'evento e verificano:

- adeguatezza dei processi decisionali;
- efficacia delle attività di coordinamento;
- correttezza delle procedure di escalation;
- efficacia delle comunicazioni interne ed esterne.

Simulazione operativa

Prevede la riproduzione controllata di uno scenario realistico che richiede l'attivazione delle procedure di continuità operativa.

L'attività consente di verificare:

- tempi di risposta;
- coordinamento delle strutture coinvolte;
- capacità di attuazione delle misure previste dal Piano;
- efficacia delle comunicazioni operative.

Test tecnico selettivo

Consiste nella verifica di specifiche componenti tecnologiche o di particolari procedure di continuità e ripristino.

Può riguardare, ad esempio:

- sistemi di backup;
- meccanismi di replica dei dati;
- strumenti di monitoraggio;
- sistemi di autenticazione e accesso;
- componenti di alta affidabilità.

Test integrato con il Piano di Disaster Recovery

È la forma più completa di verifica e coinvolge contemporaneamente aspetti organizzativi e tecnologici.

L'obiettivo è accertare l'efficacia complessiva del modello di resilienza adottato dalla Regione Piemonte attraverso la verifica coordinata di:

- attivazione del Piano di Continuità Operativa;
- processi di coordinamento e comunicazione;
- procedure di Disaster Recovery;
- recupero dei servizi e dei dati;
- raggiungimento degli obiettivi di ripristino definiti dalla BIA.

I risultati dei test sono formalizzati mediante report, evidenze e, ove necessario, azioni correttive. La pianificazione, le modalità di esecuzione, la registrazione degli esiti e la gestione delle evidenze sono disciplinate nel REGP_PR01 – Procedure per la sicurezza informatica e negli strumenti adottati dall'Ente per la relativa tracciatura.

10.1 Programma annuale

Tipo test	Frequenza minima
Walkthrough	annuale
Tabletop	annuale
Simulazione operativa	annuale
Test tecnico selettivo	annuale
Test integrato con PCO-DRP	biennale

10.2 Formazione

Il personale coinvolto nel PCO è oggetto di formazione iniziale, aggiornata periodicamente anche attraverso esercitazioni al fine di:

- garantire la conoscenza delle procedure;
- assicurare la prontezza operativa;
- migliorare la capacità di risposta agli eventi.

La pianificazione, le modalità di esecuzione e la gestione delle evidenze sono definite nel Piano di Formazione.

11 MANUTENZIONE DEL PIANO

Il Piano è riesaminato e, ove opportuno, aggiornato periodicamente e comunque almeno ogni due anni, allo scopo di verificarne l'adeguatezza, l'efficacia e la coerenza rispetto all'evoluzione del contesto organizzativo, tecnologico, normativo e dei rischi.

11.1 Riesame straordinario

Il Piano è riesaminato anticipatamente in caso di:

- modifiche significative dell'organizzazione;

- aggiornamenti della Business Impact Analysis;
- aggiornamenti del Risk Assessment;
- incidenti significativi;
- attivazione del Piano;
- risultati di test ed esercitazioni;
- mutamenti significativi dell'esposizione alle minacce e ai relativi rischi;
- variazioni normative o regolamentari.

11.2 Miglioramento continuo

Test, esercitazioni, audit, incidenti e lesson learned costituiscono input strutturati per il miglioramento continuo del sistema di continuità operativa.

12 KPI DELLA CONTINUITÀ OPERATIVA

I seguenti indicatori consentono di monitorare l'efficacia del sistema di continuità operativa e supportano le attività di riesame e miglioramento continuo.

- % servizi rilevanti coperti da BIA
- % servizi rilevanti con RTO definito
- % test eseguiti
- % azioni correttive chiuse

KPI	Descrizione	Frequenza	Obiettivo
Servizi coperti da BIA	Percentuale servizi rilevanti analizzati	Annuale	100%
Servizi con RTO definito	Copertura parametri continuità	Annuale	100%
Test eseguiti	Rispetto piano annuale	Annuale	≥ Piano annuale
Azioni correttive chiuse	Efficacia miglioramento	Semestrale	>90%

13 RACCORDI OPERATIVI E FONTI INFORMATIVE

Le informazioni e la documentazione necessarie all'attuazione del presente Piano sono mantenute, per quanto possibile, nelle fonti già previste dall'impianto documentale e operativo della Regione Piemonte, evitando la creazione e la duplicazione di allegati specifici del PCO.

In particolare:

- il REGP_REG04 – Perimetro di continuità operativa e ripristino mantiene le informazioni dinamiche condivise relative almeno al perimetro dei sistemi e servizi, ai relativi parametri di continuità e ripristino, alle priorità e alle principali dipendenze;
- il REGP_PR01 – Procedure per la sicurezza informatica disciplina le procedure operative comuni, incluse le modalità di attivazione, comunicazione, registrazione e gestione delle evidenze applicabili alla continuità operativa;

- i nominativi e i recapiti dei ruoli di sicurezza informatica sono mantenuti nelle fonti individuate nell'ambito del REGP_POL01;
- i contatti operativi, gli obblighi e i livelli di servizio dei fornitori sono mantenuti nelle fonti contrattuali e operative applicabili;
- le istruzioni tecniche e i runbook relativi ai singoli sistemi e servizi sono mantenuti dalle strutture competenti, da CSI Piemonte o dagli ulteriori soggetti gestori e sono richiamati senza duplicarne il contenuto;
- report, ticket, log, verbali e ulteriori registrazioni prodotti durante test, esercitazioni o attivazioni reali costituiscono evidenze operative e sono conservati nei sistemi e nei repository previsti per il relativo processo.

L'aggiornamento delle informazioni contenute nelle predette fonti non comporta la revisione del presente Piano, salvo che la modifica incida sugli elementi sostanziali disciplinati dal Piano stesso.

13.1 Presidi condivisi

Alcune informazioni utilizzate nell'ambito della continuità operativa sono condivise con altri documenti del sistema di resilienza.

Tali informazioni devono essere mantenute, ove possibile, mediante presidi documentali unici richiamati dai diversi piani.

Rientrano in questa categoria:

- contatti del personale e delle strutture organizzative;
- contatti dei fornitori rilevanti;
- servizi rilevanti;
- risultati della Business Impact Analysis;
- parametri RTO, RPO ed MTPD;
- modelli di comunicazione;
- report di test ed esercitazioni;
- registrazioni derivanti da eventi reali;
- action tracker e piani di miglioramento.

L'utilizzo di presidi condivisi consente di garantire uniformità delle informazioni, riduzione delle duplicazioni e semplificazione delle attività di manutenzione documentale.

PIANO DI RIPRISTINO IN CASO DI DISASTRO

Ver.	REDAZIONE		CONTROLLO APPROVAZIONE		AUTORIZZAZIONE EMISSIONE	
	NOME	DATA	NOME	DATA	NOME	DATA

STATO DELLE REVISIONI

Ver.	PARAGRAFO O PAGINA	DESCRIZIONE
	Tutto il documento	Prima versione

SOMMARIO

INDICE DELLE ABBREVIAZIONI ACN 4
PREMESSA 5
1. SCOPO E AMBITO DI APPLICAZIONE 6
1.1. Scopo 6
1.2. Ambito 7
1.3. Relazione con il sistema documentale 7
1.4. Tracciabilità rispetto ad ACN ID.IM-04 7
2. ATTIVAZIONE DEL PIANO DI RIPRISTINO 8
3. RUOLI E RESPONSABILITÀ 10
3.1. Raccordo con la matrice RACI 10
4. MODELLO OPERATIVO DI RIPRISTINO 11
5. CLASSIFICAZIONE DEI SISTEMI E PRIORITÀ DI RIPRISTINO 11
5.1. Parametri di ripristino 12
6. DIPENDENZE E PREREQUISITI 12
6.1. Categorie di dipendenza 12
6.2. Prerequisiti per il ripristino 13
7. STRATEGIE DI RIPRISTINO 13
7.1. Modello strategico di Disaster Recovery 14
7.2. Principi di applicazione delle strategie 14
7.3. Raccordo con il Piano di Continuità Operativa 15
8. PROCEDURE DI RIPRISTINO 15
8.1. Avvio delle attività di recovery 15
8.2. Esecuzione del ripristino 16
8.3. Gestione delle anomalie 16
8.4. Controllo dell'avanzamento 16
8.5. Chiusura delle attività operative 17
9. COORDINAMENTO E PARALLELISMO DELLE ATTIVITÀ 17
9.1. Gestione delle dipendenze 17
9.2. Parallelizzazione delle attività 18
9.3. Gestione delle priorità 18
9.4. Reporting e stato avanzamento 18
10. VALIDAZIONE DEL RIPRISTINO E RIENTRO A REGIME 19
10.1. Criteri di validazione 19
10.2. Verifiche di validazione 20
10.3. Rientro a regime 20

10.4. Chiusura formale del Disaster Recovery....20
11. TEST ED ESERCITAZIONI....21
11.1. Walkthrough documentale....21
11.2. Tabletop Exercise....21
11.3. Test tecnico selettivo....21
11.4. Simulazione operativa di Disaster Recovery....22
11.5. Test integrato PCO - PdGC - DRP....22
11.6. Programmazione dei test e delle esercitazioni....22
11.7. Gestione delle evidenze....23
11.8. Formazione e addestramento....23
12. TRACCIABILITÀ ED AUDIT....23
12.1. Obiettivi della tracciabilità....24
12.2. Evidenze da conservare....24
12.3. Conservazione delle evidenze....24
13. MANUTENZIONE DEL PIANO....25
13.1. Riesame ordinario....25
13.2. Riesame straordinario....26
13.3. Gestione delle modifiche....26
13.4. Miglioramento continuo....27
14. KPI DEL DISASTER RECOVERY....27
14.1. Obiettivi del monitoraggio....28
14.2. Indicatori di prestazione....28
14.3. Analisi dei risultati....28
14.4. Reporting direzionale....28
14.5. Gestione delle non conformità e delle azioni correttive....29
15. RACCORDI OPERATIVI E FONTI INFORMATIVE....29

INDICE DELLE ABBREVIAZIONI ACN

BCP *Business Continuity Plan*
BIA *Business Impact Analysis*
CISO *Chief Information Security Officer*
CIO *Chief Information Officer*
CSIRT *Computer Security Incident Response Team*
DR *Disaster Recovery*
ICT *Information and Communication Technology*
ID.IM *Identify - Incident Management*
IRT *Incident Response Team*
NIS2 *Direttiva (UE) 2022/2555 sulla cybersicurezza*
RPO *Recovery Point Objective*
RTO *Recovery Time Objective*
MTPD *Maximum Tolerable Period of Disruption*
SIEM *Security Information and Event Management*
SLA *Service Level Agreement*
SOC *Security Operations Center*

PREMESSA

La Regione Piemonte eroga e supporta un insieme articolato di servizi digitali destinati ai cittadini, alle imprese, agli enti territoriali, al sistema sanitario regionale e alle strutture dell'Amministrazione regionale. La disponibilità, l'integrità e la resilienza dei sistemi informativi e di rete che supportano tali servizi rappresentano un elemento essenziale per garantire il corretto svolgimento delle funzioni istituzionali e la continuità dei servizi pubblici.

L'evoluzione delle minacce cyber, la crescente interconnessione tra piattaforme digitali, l'utilizzo di infrastrutture condivise e servizi cloud e la dipendenza da fornitori esterni rendono necessario adottare un modello strutturato di Disaster Recovery in grado di garantire il ripristino tempestivo delle funzionalità tecnologiche in caso di eventi avversi.

Il presente Piano di Ripristino in caso di Disastro (Disaster Recovery Plan - DRP) definisce il quadro organizzativo, metodologico e operativo adottato dalla Regione Piemonte per il recupero delle infrastrutture, delle piattaforme tecnologiche, dei dati e dei servizi digitali rilevanti a seguito di eventi che ne compromettano la disponibilità.

Il Piano è redatto in conformità alla Direttiva (UE) 2022/2555 (NIS2), al D.Lgs. 138/2024 e alle indicazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN), con particolare riferimento alle misure previste nell'ambito ID.IM-04 relative alla continuità operativa, alla gestione delle crisi e al ripristino dei servizi.

Il DRP costituisce parte integrante del sistema di resilienza organizzativa e digitale della Regione Piemonte e deve essere letto congiuntamente agli altri documenti che concorrono alla gestione della sicurezza e della continuità operativa dell'Ente.

Il presente Piano costituisce il documento di indirizzo e pianificazione strategica in materia di ripristino in caso di disastro dei sistemi informativi e di rete rilevanti. Esso è sottoposto all’approvazione degli organi amministrativi e direttivi competenti ai sensi del quadro normativo NIS e delle misure di sicurezza di base ACN, con particolare riferimento a ID.IM-04 punto 4.
Il dettaglio operativo necessario all’attuazione del presente Piano è disciplinato, per le modalità procedurali comuni, nel REGP_PR01 – Procedure per la sicurezza informatica e, per le attività tecniche riferite a specifici sistemi o servizi, nei runbook, nelle checklist e nelle istruzioni tecniche mantenute dalle strutture competenti, da CSI Piemonte o dagli ulteriori soggetti gestori. Le registrazioni e le evidenze prodotte durante le attività sono mantenute nei sistemi e nei repository previsti per il relativo processo.

In particolare, il Piano si integra con:

- la Business Impact Analysis (BIA), che individua i servizi rilevanti e definisce gli obiettivi di continuità;
- il Risk Assessment, che identifica e valuta i rischi che possono compromettere la disponibilità dei servizi;
- il Piano di Continuità Operativa (PCO), che definisce strategie, priorità e misure organizzative;
- il Piano di Gestione delle Crisi (PdGC), che disciplina i processi decisionali e la governance degli eventi di particolare gravità;

- il Piano di Gestione degli Incidenti, che regola le attività di gestione operativa degli eventi e degli incidenti di sicurezza.

Il presente Piano si applica almeno ai sistemi informativi e di rete rilevanti individuati dalla Regione Piemonte, tenendo conto degli esiti della Business Impact Analysis, delle valutazioni del rischio e delle ulteriori informazioni utilizzate dall'Ente per la definizione delle esigenze di ripristino.
Il Piano contribuisce all'attuazione coordinata delle misure di continuità operativa, gestione della crisi e resilienza digitale adottate dalla Regione Piemonte.

1. SCOPO E AMBITO DI APPLICAZIONE

1.1. Scopo

Il presente Piano di Ripristino in caso di Disastro ha lo scopo di definire il quadro di riferimento per il recupero dei sistemi informativi e di rete rilevanti della Regione Piemonte, in seguito a eventi che ne compromettano la disponibilità in modo totale o parziale.

In particolare, il Piano ha la finalità di:

- garantire il ripristino dei sistemi informativi e di rete rilevanti entro i tempi definiti dagli obiettivi di Recovery Time Objective (RTO);
- assicurare il recupero delle informazioni e dei dati entro i limiti di perdita definiti dai Recovery Point Objective (RPO);
- minimizzare gli impatti derivanti dall'indisponibilità dei servizi digitali;
- assicurare il coordinamento delle attività tecniche di recovery;
- garantire la corretta gestione delle dipendenze tra sistemi, applicazioni, infrastrutture e fornitori;
- assicurare la tracciabilità delle attività di ripristino e delle decisioni adottate;
- contribuire al rispetto degli obblighi normativi e regolamentari in materia di cybersicurezza e resilienza operativa.

Il Piano definisce il quadro strategico e metodologico per il ripristino dei sistemi informativi e di rete rilevanti. Le modalità procedurali comuni sono disciplinate nel REGP_PR01 – Procedure per la sicurezza informatica; le modalità tecniche di esecuzione sono demandate ai runbook e alla documentazione tecnica mantenuta dalle strutture competenti, da CSI Piemonte o dagli ulteriori soggetti gestori.

Restano disciplinati da documenti separati:

- la gestione della crisi e dei processi decisionali straordinari, regolata dal Piano di Gestione delle Crisi;
- le strategie organizzative di continuità operativa, definite dal Piano di Continuità Operativa;
- la gestione degli incidenti e delle emergenze operative, regolata dal Piano di Gestione degli Incidenti.

Il Piano è soggetto a riesame periodico e aggiornamento in occasione di variazioni significative dei sistemi, dei servizi o del contesto normativo.
Il Piano individua, a livello di indirizzo e pianificazione, criteri di attivazione, ruoli, responsabilità, priorità, principi di recovery, modalità di validazione, evidenze e obblighi di riesame. Le istruzioni operative di

dettaglio sono richiamate come presidi attuativi e possono essere aggiornate con maggiore frequenza per recepire cambiamenti tecnici, organizzativi o tecnologici.

1.2. **Ambito**

Il Piano si applica:

- ai sistemi informativi e di rete rilevanti ai sensi della normativa NIS2;
- ai servizi per i quali sono state effettuate le analisi di BIA e Risk Assessment.

Sono destinatari del Piano le strutture regionali, le figure operative e i soggetti esterni coinvolti, secondo le rispettive competenze, nelle attività di pianificazione, coordinamento ed esecuzione del ripristino.

Per l'individuazione dei ruoli dell'organizzazione per la sicurezza informatica e delle relative responsabilità si rinvia al **REGP_POL01 - Modello per la Sicurezza Informatica**; le responsabilità specifiche relative all'esecuzione del presente Piano sono definite nel capitolo 3.

L'elenco vigente dei sistemi e dei servizi compresi nel perimetro, con i relativi parametri di continuità e ripristino e le principali dipendenze, è mantenuto nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

1.3. **Relazione con il sistema documentale**

Il presente Piano si inserisce nel sistema documentale della Regione Piemonte dedicato alla resilienza organizzativa e digitale e deve essere applicato in coordinamento con i documenti correlati.

Documento	Finalità
Business Impact Analysis	Identificazione dei servizi rilevanti e definizione di RTO, RPO e MTPD
Risk Assessment	Valutazione dei rischi
Piano Gestione Incidenti	Gestione operativa degli eventi
Piano Continuità Operativa	Strategie di continuità
Piano di Gestione delle Crisi	Governance e processi decisionali
Piano di Ripristino in caso di Disastro	Ripristino tecnologico
REGP_PR01 – Procedure per la sicurezza informatica	Procedure operative comuni per l'attuazione dei piani e dei processi di sicurezza informatica
REGP_POL01 – Organizzazione per la sicurezza informatica	Assetto organizzativo, ruoli, responsabilità e raccordi organizzativi
REGP_REG04 – Perimetro di continuità operativa e ripristino	Perimetro, parametri di continuità e ripristino, priorità, dipendenze e riferimenti operativi

1.4. **Tracciabilità rispetto ad ACN ID.IM-04**

Il presente Piano contribuisce alla copertura dei requisiti previsti dalla misura ACN ID.IM-04 relativamente agli aspetti di disaster recovery, continuità operativa e resilienza dei sistemi informativi e di rete rilevanti.

Il presente Piano assicura la tracciabilità dei contenuti richiesti dal punto 2 della misura ACN ID.IM-04 secondo la seguente corrispondenza:

Requisito ID.IM-04	Copertura documentale
a) Finalità, esigenze di ripristino e ambito di applicazione	Premessa; §§ 1.1 e 1.2
b) Ruoli e responsabilità	Cap. 3; REGP_POL01 per l'assetto organizzativo generale
c) Contatti principali e canali di comunicazione interni ed esterni	§ 3.1; REGP_POL01; fonte nominativa vigente dell'Ente; REGP_PR01 e documenti di gestione degli incidenti e delle crisi per i rispettivi flussi
d) Condizioni di attivazione e disattivazione	Cap. 2 e § 10.4
e) Risorse necessarie, inclusi backup e ridondanze	Capp. 6 e 7; REGP_REG04; documentazione tecnica e contrattuale applicabile
f) Ordine di ripristino delle operazioni	Cap. 5 e § 9.3; REGP_REG04
g) Procedure di ripristino per operazioni specifiche e relativi obiettivi	Capp. 7, 8 e 10; REGP_PR01 e runbook tecnici applicabili

Il Piano è approvato dagli organi di amministrazione e direttivi competenti e sottoposto a riesame secondo quanto previsto dal capitolo 13.

2. ATTIVAZIONE DEL PIANO DI RIPRISTINO

L'attivazione del Piano di Ripristino in caso di Disastro avviene a seguito della valutazione di un evento che abbia compromesso o possa compromettere la disponibilità dei sistemi informativi e di rete rilevanti e che richieda l'attivazione di procedure straordinarie di recupero tecnologico.

La valutazione è effettuata tenendo conto dei seguenti fattori:

- criticità del servizio coinvolto;
- impatti sulle funzioni istituzionali;
- durata prevista dell'interruzione;
- rischio di superamento degli obiettivi RTO;
- rischio di perdita dati superiore agli obiettivi RPO;
- numero di servizi coinvolti;
- coinvolgimento di dipendenze critiche;
- indisponibilità di infrastrutture condivise;
- necessità di attivare processi di escalation.

L'attivazione può essere proposta dalle strutture tecniche o organizzative competenti in relazione al servizio e all'evento interessato e può essere disposta, secondo le competenze organizzative vigenti dell'Ente, anche in via preventiva qualora siano presenti condizioni che possano verosimilmente determinare l'indisponibilità dei servizi rilevanti.

La dichiarazione dello stato di crisi e l'eventuale attivazione del Piano di Gestione delle Crisi restano disciplinate dal relativo documento.

L'attivazione del Piano può avvenire anche a seguito di segnalazioni provenienti da fornitori critici, CSIRT Italia, ACN o altre autorità competenti.
Quando l'evento che determina l'attivazione del DRP ha natura cyber o può configurare un incidente significativo ai fini NIS, il processo di ripristino è coordinato con il Piano di Gestione degli Incidenti. Il Punto di contatto NIS2 e il Referente CSIRT intervengono secondo le rispettive competenze definite dal REGP_POL01 e dalla documentazione di gestione degli incidenti, rispettivamente per le comunicazioni verso l'Autorità nazionale competente NIS e per le interlocuzioni e notifiche verso lo CSIRT Italia.
Le attività di recovery non devono compromettere la conservazione delle evidenze utili all'analisi dell'incidente, alla ricostruzione degli eventi, alla valutazione degli impatti e all'eventuale adempimento degli obblighi di notifica.

Livelli di attivazione

Livello	Descrizione	Effetto	Esempio
0	Incidente	Gestione ordinaria	Guasto circoscritto di un singolo servizio
1	Recovery locale	Attivazione procedure di ripristino limitate	Ripristino applicativo da backup
2	Grave indisponibilità	Coordinamento strutturato delle attività di recovery	Superamento RTO previsto
3	Disastro	Attivazione del DRP e valutazione dell'eventuale attivazione del Piano di gestione delle crisi secondo i relativi criteri	Indisponibilità estesa di infrastrutture o sistemi rilevanti

Processo di attivazione

Le fasi iniziali di valutazione tecnica e analisi degli impatti possono svolgersi nell'ambito della gestione ordinaria degli eventi e degli incidenti. La decisione di attivazione del DRP è assunta secondo le responsabilità definite nel presente Piano. Qualora ricorrano i criteri previsti dal PdGC, l'attivazione e l'esecuzione del DRP sono coordinate con la gestione della crisi. Il DRP può pertanto essere attivato anche in assenza dell'attivazione del PdGC.

Fase	Attività	Raccordo con PdGC
1	Segnalazione evento	Gestione ordinaria dell'evento o dell'incidente
2	Valutazione tecnica	Gestione dell'incidente e raccolta delle informazioni
3	Analisi impatti e obiettivi di ripristino	Valutazione dell'eventuale rilevanza ai fini della crisi
4	Decisione di attivazione	Se ricorrono i criteri previsi dal PdGC, contestuale proposta o decisione di attivazione PdGC
5	Convocazione del team di recovery	DRP attivo; coordinamento con il Comitato di Crisi se il PdGC è attivato
6	Avvio delle procedure di ripristino	Esecuzione del DRP; raccordo con il PdGC ove attivato
7	Monitoraggio e reporting	Flussi informativi verso i responsabili competenti e, ove attivato, verso il Comitato di Crisi

3. RUOLI E RESPONSABILITÀ

L'assetto generale dei ruoli, delle responsabilità e dei raccordi organizzativi in materia di cybersicurezza è definito nel **REGP_POL01 – Organizzazione per la Sicurezza Informatica**, che costituisce il riferimento organizzativo unitario dell'Ente. Il presente Piano non ridefinisce tale assetto e disciplina esclusivamente le responsabilità specifiche connesse alle attività di ripristino.

Per i profili specificamente attinenti alla cybersicurezza, il presidio tecnico-organizzativo delle attività di continuità e ripristino è assicurato dal **Settore A1911A - Sistema informativo regionale**, in raccordo con il **Settore A1910A - Servizi infrastrutturali e tecnologici** e con le altre strutture regionali competenti.

Le strutture competenti per i servizi interessati concorrono alla definizione delle priorità di recupero e alla validazione del ripristino per gli ambiti di rispettiva competenza.

I team tecnici, i fornitori, gli eventuali soggetti in house e le altre terze parti coinvolte eseguono le attività tecniche di recovery di rispettiva competenza secondo i runbook, i contratti, le convenzioni, i disciplinari e gli accordi di servizio applicabili.

Ai fini del presente Piano, l'espressione **"DR Manager"**, ove utilizzata nei successivi paragrafi e nei presidi operativi, identifica esclusivamente la **funzione operativa di coordinamento delle attività di recovery** e non costituisce un ulteriore ruolo organizzativo permanente rispetto a quelli definiti dal REGP_POL01. Tale funzione è esercitata nell'ambito delle strutture competenti e nel rispetto dell'assetto organizzativo vigente.

Qualora l'evento abbia natura cyber, il Punto di contatto NIS2 e il Referente CSIRT intervengono esclusivamente nell'ambito delle rispettive attribuzioni definite dal REGP_POL01 e dal Piano di Gestione degli Incidenti.

Qualora sia attivato il Piano di Gestione delle Crisi, i ruoli decisionali e i relativi meccanismi di governance sono quelli definiti dal medesimo Piano e non sono ridefiniti nel presente documento.

Il presente Piano è approvato dagli organi di amministrazione e direttivi competenti secondo quanto previsto dalla disciplina NIS e dall'assetto organizzativo dell'Ente.

3.1. Raccordo con la matrice RACI

Il presente Piano non introduce una matrice RACI organizzativa autonoma rispetto al REGP_POL01. Le responsabilità generali sono quelle definite dall'organizzazione dell'Ente; l'attribuzione delle singole attività tecniche di recovery è riportata, ove necessario, nei runbook e nella documentazione operativa applicabile ai sistemi e ai servizi interessati.

I nominativi e i recapiti relativi ai ruoli di sicurezza informatica sono mantenuti nella fonte nominativa vigente dell'Ente. I riferimenti operativi relativi ai servizi e ai soggetti gestori sono mantenuti nelle fonti organizzative, contrattuali e operative applicabili e, ove pertinente, richiamati nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

I canali e i flussi di comunicazione in materia di cybersicurezza sono quelli definiti dal REGP_POL01 e, in relazione alla natura dell'evento, dal Piano di Gestione degli Incidenti e dal Piano di Gestione delle Crisi. I runbook e i presidi operativi possono individuare ulteriori canali tecnici necessari al coordinamento delle attività di recovery.

Per i servizi gestiti da fornitori o soggetti in house, le responsabilità operative e i relativi canali di escalation sono quelli definiti dai contratti, dalle convenzioni, dagli accordi di servizio e dalla documentazione operativa applicabile.

4. MODELLO OPERATIVO DI RIPRISTINO

Il modello operativo di Disaster Recovery adottato dalla Regione Piemonte descrive il processo attraverso il quale un evento che compromette la disponibilità di sistemi, infrastrutture o dati viene gestito fino al completo ripristino delle condizioni operative attese.

L'obiettivo del modello è garantire:

- chiarezza delle responsabilità;
- tracciabilità delle attività svolte;
- corretta gestione delle dipendenze tecniche;
- rispetto di RTO e RPO;
- validazione controllata del ripristino;
- raccolta delle evidenze necessarie ai fini di audit e miglioramento continuo.

Il processo di Disaster Recovery si articola nelle fasi riportate nella tabella seguente.

Rilevazione Evento, incidente, allarme → Segnalazione	→	**Valutazione** Analisi impatti e criticità → Decisione di attivazione	→	**Attivazione** DRP attivato → Team di recovery operativo
Ripristino Procedure e runbook → Recupero progressivo servizi	→	**Validazione** Test e verifiche → Conferma funzionalità	→	**Rientro a regime** Servizi stabilizzati → Chiusura recovery
Lesson Learned → Evidenze e report → Miglioramenti				

Durante tutte le fasi del processo devono essere mantenute informazioni aggiornate sullo stato di avanzamento, sulle attività completate, sulle criticità riscontrate e sulle eventuali azioni correttive necessarie.

Le attività di Disaster Recovery possono essere svolte in modalità sequenziale o parallela in funzione delle dipendenze tecniche esistenti e delle priorità di recupero definite dal presente Piano.

5. CLASSIFICAZIONE DEI SISTEMI E PRIORITÀ DI RIPRISTINO

La definizione delle priorità di ripristino rappresenta un elemento essenziale del Disaster Recovery e consente di assicurare che le risorse disponibili siano impiegate prioritariamente per il recupero dei servizi maggiormente rilevanti per la Regione Piemonte.

Le priorità sono determinate attraverso le attività di classificazione dei servizi, Business Impact Analysis e Risk Assessment e tengono conto degli impatti associati all'indisponibilità dei servizi digitali e delle funzioni istituzionali supportate.

Per ciascun sistema o servizio rilevante sono definiti:

- livello di criticità;
- Recovery Time Objective (RTO);
- Recovery Point Objective (RPO);
- Maximum Tolerable Period of Disruption (MTPD);
- dipendenze critiche;
- ordine di recupero.

La classificazione dei sistemi e dei servizi rilevanti è riesaminata periodicamente nell'ambito delle attività di Business Impact Analysis e Risk Assessment e costituisce il principale riferimento per la definizione delle priorità di recovery.

5.1. **Parametri di ripristino**

I parametri **RTO, RPO, MTPD e livello di criticità** sono determinati nell'ambito della Business Impact Analysis e richiamati dal Piano di Continuità Operativa; il presente Piano ne utilizza i valori vigenti senza duplicarne la definizione.

Ai fini del Disaster Recovery:

- l'RTO costituisce riferimento per la definizione dei tempi e delle priorità di ripristino;
- l'RPO orienta le strategie di backup, replica e recupero dei dati;
- l'MTPD costituisce il limite massimo di indisponibilità da considerare nella pianificazione;
- il livello di criticità, unitamente alle dipendenze tra sistemi e servizi, concorre alla determinazione dell'ordine di recupero.

I valori applicabili ai singoli sistemi e servizi, unitamente alle relative priorità e alle principali dipendenze, sono mantenuti nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

6. **DIPENDENZE E PREREQUISITI**

La capacità della Regione Piemonte di ripristinare i servizi digitali dipende dalla disponibilità di infrastrutture, competenze, risorse e soggetti esterni che concorrono all'erogazione dei servizi.

L'identificazione preventiva delle dipendenze costituisce un requisito fondamentale per la pianificazione delle attività di Disaster Recovery e permette di ridurre i tempi necessari al recupero dei sistemi e dei dati.

Per ciascun sistema o servizio rilevante vengono identificate e mantenute aggiornate le principali dipendenze tecnologiche, organizzative ed esterne.

6.1. **Categorie di dipendenza**

Categoria	Descrizione	Esempi
Dipendenze	Componenti infrastrutturali necessarie	Data Center, cloud, reti dati, sistemi IAM, sistemi

Categoria	Descrizione	Esempi
tecnologiche	all'erogazione del servizio	di backup
Dipendenze organizzative	Competenze e strutture necessarie alla gestione del servizio	Team specialistici, responsabili applicativi, supporto sistemistico
Dipendenze esterne	Risorse e servizi erogati da soggetti terzi	CSI Piemonte, cloud provider, TLC, PEC, conservazione digitale

6.2. Prerequisiti per il ripristino

Prima dell'avvio delle procedure di Disaster Recovery devono risultare disponibili, ove applicabili:

- personale tecnico identificato e reperibile;
- accessi amministrativi e credenziali di emergenza;
- documentazione tecnica aggiornata;
- runbook operativi;
- backup utilizzabili e verificati;
- infrastrutture alternative previste dalle strategie di recovery;
- collegamenti di rete necessari alle attività di recupero;
- supporto dei fornitori coinvolti.

L'assenza di uno o più prerequisiti deve essere immediatamente registrata e gestita attraverso le procedure di escalation previste dal presente Piano.

Per ciascuna dipendenza critica, ove applicabile, sono considerate misure di mitigazione, modalità di escalation e soluzioni alternative. Il dettaglio delle dipendenze e dei prerequisiti riferiti ai singoli sistemi e servizi è mantenuto nel REGP_REG04 – Perimetro di continuità operativa e ripristino.
Per i fornitori rilevanti e per le dipendenze esterne critiche devono essere definiti, ove applicabile, requisiti coerenti con gli obiettivi di recovery del presente Piano, inclusi livelli di servizio, tempi di presa in carico, modalità di escalation, contatti di emergenza, obblighi di collaborazione durante incidenti e disastri, disponibilità di evidenze tecniche e partecipazione ai test o alle esercitazioni di competenza.
La coerenza tra SLA, obblighi contrattuali e valori RTO/RPO deve essere verificata in sede di riesame del Piano e in occasione di modifiche significative ai servizi, ai contratti o alle architetture tecnologiche.

7. STRATEGIE DI RIPRISTINO

Le strategie di Disaster Recovery adottate dalla Regione Piemonte sono definite sulla base delle risultanze della Business Impact Analysis, delle attività di Risk Assessment, della classificazione dei servizi e delle caratteristiche delle infrastrutture che supportano l'erogazione dei servizi digitali regionali.

Le strategie di ripristino hanno l'obiettivo di garantire il recupero tempestivo dei sistemi informativi e di rete rilevanti, minimizzando gli impatti operativi, economici, organizzativi e normativi derivanti da eventi che ne compromettano la disponibilità.

La scelta delle strategie di recovery tiene conto in particolare di:

- livello di criticità del servizio;
- valori di RTO e RPO assegnati;
- dipendenze tecnologiche;
- disponibilità di infrastrutture alternative;
- sostenibilità economica delle misure adottate;
- obblighi normativi applicabili;
- esigenze di continuità operativa dei servizi istituzionali.

Le strategie individuate costituiscono il quadro complessivo di riferimento per la predisposizione delle procedure operative di ripristino e dei relativi runbook tecnici.

7.1. Modello strategico di Disaster Recovery

La Regione Piemonte adotta un modello multilivello di Disaster Recovery che combina misure organizzative e tecnologiche finalizzate a garantire differenti livelli di resilienza in funzione della criticità dei servizi.

Strategia	Obiettivo	Applicazione
Backup Restore	Recupero dei dati e dei sistemi mediante ripristino da copie di sicurezza	Sistemi ordinari e servizi non critici
Replica dati	Riduzione della perdita potenziale di dati	Servizi critici con RPO ridotto
Site Recovery	Attivazione di infrastrutture alternative	Infrastrutture condivise e servizi ad alta criticità
Rebuild Infrastructure	Ricostruzione controllata dell'ambiente compromesso	Compromissione infrastrutturale o cyber
Cloud Recovery	Ripristino da ambienti cloud o servizi gestiti	Servizi ospitati in cloud
Recovery tramite fornitore	Ripristino effettuato con il supporto di terze parti specializzate	Servizi esternalizzati

7.2. Principi di applicazione delle strategie

Le strategie di ripristino devono essere applicate secondo i seguenti principi:

Prioritizzazione
Le attività di ripristino devono tenere conto dell'ordine di priorità risultante dalla Business Impact Analysis e mantenuto nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

Proporzionalità
Le risorse impiegate per il ripristino devono essere proporzionate alla criticità del servizio e alla gravità dell'evento che ha determinato l'attivazione del Piano.

Tracciabilità
Ogni attività eseguita durante il ripristino deve essere registrata, documentata e conservata quale evidenza delle operazioni effettuate.

Sicurezza

Le attività di recovery devono essere svolte garantendo il mantenimento dei requisiti di sicurezza delle informazioni e delle misure di protezione previste dalla Regione Piemonte.

7.3. Raccordo con il Piano di Continuità Operativa

Le strategie di Disaster Recovery costituiscono l'attuazione tecnica delle priorità e degli obiettivi definiti nel Piano di Continuità Operativa.

Il Piano di Continuità Operativa definisce infatti:

- servizi prioritari;
- ambiti di continuità;
- livelli di criticità;
- obiettivi di resilienza.

Il presente Piano definisce invece le modalità tecniche necessarie al recupero delle infrastrutture, delle piattaforme, dei sistemi e dei dati che consentono l'erogazione dei servizi individuati come rilevanti.

La strategia di ripristino applicabile ai singoli servizi è definita sulla base della BIA, delle analisi di rischio, dei valori RTO/RPO e delle caratteristiche delle soluzioni tecnologiche adottate; il relativo riferimento è mantenuto nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

8. PROCEDURE DI RIPRISTINO

Le procedure di ripristino disciplinano l'esecuzione operativa delle attività necessarie per recuperare sistemi, infrastrutture e dati a seguito dell'attivazione del Disaster Recovery Plan.

Il presente capitolo descrive il processo comune di ripristino e i relativi criteri di controllo. Le modalità procedurali comuni sono disciplinate anche nel REGP_PR01 – Procedure per la sicurezza informatica; il dettaglio esecutivo, incluse sequenze tecniche, comandi, configurazioni e checklist di sistema, è disciplinato nei runbook e nella documentazione tecnica applicabile ai singoli sistemi e servizi.

I runbook sono mantenuti dalle strutture competenti, da CSI Piemonte o dagli ulteriori soggetti gestori e sono richiamati, ove necessario, nel REGP_REG04 – Perimetro di continuità operativa e ripristino, senza essere allegati al presente Piano.

8.1. Avvio delle attività di recovery

A seguito dell'attivazione del DRP il DR Manager:

- conferma il perimetro dei sistemi coinvolti;
- verifica le priorità di recupero;

identifica le risorse infrastrutturali, tecnologiche, organizzative e professionali necessarie al ripristino;

- verifica la disponibilità dei fornitori coinvolti;

- dispone l'avvio delle procedure previste dai runbook.

L'avvio delle attività deve essere tracciato negli strumenti utilizzati per la gestione del recovery, secondo quanto previsto dal REGP_PR01 – Procedure per la sicurezza informatica.

8.2. **Esecuzione del ripristino**

Le attività di ripristino sono definite nei runbook e nei presidi operativi applicabili al sistema o servizio interessato. Le attività di seguito riportate costituiscono esempi di operazioni che possono essere eseguite nell'ambito di un processo di Disaster Recovery e non rappresentano un elenco esaustivo né obbligatorio per ogni scenario di ripristino.

- Recupero da backup;
- riattivazione di sistemi virtuali;
- riallineamento delle repliche;
- ripristino database;
- recupero delle configurazioni;
- ricostruzione di ambienti compromessi;
- attivazione di infrastrutture alternative;
- ripristino dei collegamenti di rete;
- verifica delle interdipendenze applicative.

Durante l'esecuzione delle attività di recovery devono essere mantenuti controlli minimi di sicurezza, inclusi il tracciamento degli accessi amministrativi, la verifica dell'integrità dei backup utilizzati, la segregazione degli ambienti compromessi, la protezione delle evidenze e il coordinamento con i team di sicurezza in caso di evento cyber.

Le procedure operative devono essere eseguite esclusivamente da personale autorizzato e secondo le istruzioni contenute nei rispettivi runbook.

8.3. **Gestione delle anomalie**

Qualora durante il processo di recovery emergano anomalie che possano compromettere il rispetto degli obiettivi di ripristino, il responsabile dell'attività deve:

- registrare l'anomalia;
- valutare gli impatti sui tempi di recupero;
- informare il DR Manager;
- attivare eventuali escalation tecniche;
- proporre azioni alternative.

Tutte le anomalie devono essere documentate e riportate nella reportistica finale dell'evento.

8.4. **Controllo dell'avanzamento**

Durante l'esecuzione delle attività di ripristino devono essere monitorati almeno i seguenti elementi:

Elemento	Obiettivo
Stato procedure	Verificare il completamento delle attività
Tempi di recovery	Monitorare rispetto RTO
Recupero dati	Monitorare rispetto RPO
Dipendenze	Coordinare attività correlate
Criticità aperte	Gestire eventuali blocchi

Il monitoraggio deve proseguire fino al completamento delle attività di recovery.

8.5. Chiusura delle attività operative

Le attività operative di recovery sono considerate concluse quando:

- tutte le procedure previste sono state completate;
- sono state effettuate le verifiche tecniche previste;
- sono stati raccolti gli elementi di evidenza richiesti;
- sono stati resi disponibili ai Responsabili dei servizi gli elementi necessari all'esecuzione delle attività di validazione.

L'eventuale mancato superamento della validazione determina la riapertura o la prosecuzione delle attività di recovery e la registrazione della relativa anomalia secondo quanto previsto dal paragrafo 8.3.

La chiusura tecnica delle attività costituisce prerequisito per la successiva dichiarazione di completamento del ripristino.

Le procedure tecniche dettagliate sono contenute nei runbook e nella documentazione tecnica mantenuti dalle strutture competenti o dai soggetti gestori. Il relativo riferimento è mantenuto, ove pertinente, nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

9. COORDINAMENTO E PARALLELISMO DELLE ATTIVITÀ

Le attività di Disaster Recovery coinvolgono frequentemente sistemi tra loro interdipendenti, infrastrutture condivise e fornitori esterni. Per tale motivo il coordinamento centralizzato delle operazioni costituisce un elemento essenziale per garantire l'efficacia del ripristino.

Il coordinamento operativo è svolto dal DR Manager che assicura la gestione delle priorità, il monitoraggio dello stato di avanzamento e la corretta allocazione delle risorse disponibili.

9.1. Gestione delle dipendenze

Prima dell'esecuzione delle attività di recovery devono essere identificate e valutate le dipendenze esistenti tra:

- piattaforme infrastrutturali;

- sistemi di autenticazione;
- servizi di rete;
- basi dati;
- applicazioni;
- servizi cloud;
- fornitori rilevanti.

L'ordine di esecuzione delle procedure deve tenere conto delle dipendenze individuate per evitare ritardi o attività non efficaci.

9.2. **Parallelizzazione delle attività**

Ove tecnicamente possibile le attività di recovery possono essere eseguite in parallelo al fine di ridurre i tempi complessivi di ripristino.

La parallelizzazione può riguardare:

- recupero di più server contemporaneamente;
- ripristino simultaneo di ambienti applicativi;
- attività svolte da team diversi;
- interventi su infrastrutture indipendenti;
- attività svolte dai fornitori.

La parallelizzazione deve essere autorizzata dal DR Manager e non deve compromettere il controllo delle attività o l'integrità dei dati recuperati.

Quando prevista dai runbook approvati, la parallelizzazione non richiede una specifica autorizzazione per la singola esecuzione. Le decisioni di parallelizzazione non già previste dai runbook devono essere autorizzate dal DR Manager e registrate nel registro delle attività, unitamente alle relative motivazioni e agli eventuali vincoli.

9.3. **Gestione delle priorità**

In presenza di risorse limitate le attività devono essere indirizzate prioritariamente verso:

1. sistemi informativi e di rete rilevanti
2. sistemi di autenticazione e sicurezza;
3. servizi classificati strategici;
4. servizi classificati critici;
5. servizi classificati come ordinari.

La priorità effettiva delle attività deve essere verificata sulla base dei parametri, delle dipendenze e dell'ordine di ripristino mantenuti nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

9.4. **Reporting e stato avanzamento**

Durante il Disaster Recovery devono essere prodotti aggiornamenti periodici contenenti:

- attività completate;
- attività in corso;
- criticità riscontrate;
- ritardi rispetto alla pianificazione;
- previsioni di completamento;
- eventuali richieste di escalation.

I report costituiscono parte integrante delle evidenze dell'evento e devono essere conservati secondo le modalità previste dal presente Piano.

La frequenza della reportistica è determinata dal livello di gravità dell'evento e dalle esigenze informative dei soggetti coinvolti.

Le modalità di registrazione e reporting sono disciplinate nel REGP_PR01 – Procedure per la sicurezza informatica e possono avvalersi dei modelli, delle checklist e degli strumenti già utilizzati dalle strutture competenti o dai soggetti gestori.

10. VALIDAZIONE DEL RIPRISTINO E RIENTRO A REGIME

I criteri descritti nel presente capitolo riguardano esclusivamente il completamento del processo di Disaster Recovery e non sostituiscono gli eventuali criteri di chiusura della crisi previsti dal PdGC.

La conclusione delle attività tecniche di Disaster Recovery non coincide automaticamente con il completamento del processo di ripristino.

Affinché il ripristino possa essere dichiarato completato è necessario verificare che i sistemi, le applicazioni, le infrastrutture e i dati coinvolti abbiano recuperato un livello di funzionalità coerente con i requisiti definiti dalla Regione Piemonte e con gli obiettivi individuati nell'ambito della Business Impact Analysis.

La fase di validazione ha lo scopo di garantire che il servizio ripristinato sia effettivamente disponibile, utilizzabile e conforme ai livelli minimi accettabili definiti dall'organizzazione. Essa costituisce inoltre un elemento fondamentale ai fini della tracciabilità delle attività svolte e della raccolta delle evidenze richieste per audit, verifiche e miglioramento continuo.

10.1. Criteri di validazione

Per poter dichiarare completato il ripristino devono risultare soddisfatti almeno i seguenti criteri:

- completamento delle attività tecniche previste dai runbook;
- disponibilità operativa delle infrastrutture coinvolte;
- disponibilità dei servizi applicativi interessati in coerenza con i livelli di servizio definiti dalla Business Impact Analysis;
- verifica dell'integrità dei dati recuperati;
- verifica dei log rilevanti;
- assenza di anomalie bloccanti;
- completamento dei controlli di sicurezza previsti;
- verifica degli eventi di sicurezza connessi all’incidente;
- conferma del rispetto degli obiettivi di recovery applicabili;

- assenza di compromissioni residue note che impediscano il ripristino sicuro del servizio, oppure formale accettazione e gestione del rischio residuo secondo i processi competenti.

Qualora uno o più criteri non risultino soddisfatti il processo di recovery deve proseguire fino alla risoluzione delle criticità individuate.

10.2. Verifiche di validazione

Le verifiche devono essere eseguite in modo proporzionato alla criticità del sistema e alla complessità delle attività effettuate.

Verifica	Obiettivo
Test infrastrutturale	Verificare disponibilità delle componenti tecnologiche
Test applicativo	Verificare corretto funzionamento delle applicazioni
Test di accesso	Verificare autenticazione e autorizzazioni
Verifica dati	Verificare completezza e integrità delle informazioni
Test di integrazione	Verificare interazioni tra sistemi

10.3. Rientro a regime

A seguito della validazione del ripristino viene avviata la fase di rientro a regime.

Le attività possono comprendere:

- disattivazione delle configurazioni temporanee;
- riallineamento degli ambienti operativi;
- riattivazione delle attività sospese;
- aggiornamento della documentazione operativa e delle evidenze prodotte durante l'evento;
- chiusura delle procedure straordinarie;
- trasferimento della gestione ai processi ordinari.

L'obiettivo della fase di rientro è garantire il ritorno alle normali condizioni operative minimizzando il rischio di ulteriori interruzioni o anomalie.

10.4. Chiusura formale del Disaster Recovery

La chiusura formale del Disaster Recovery è disposta dal DR Manager a seguito della verifica del completamento delle attività previste e dell'esito della validazione del ripristino.
Prima della chiusura devono essere disponibili:

Evidenza	Contenuto
Registro attività	Cronologia delle operazioni svolte
Report di recovery	Sintesi delle attività eseguite
Evidenze tecniche	Log, screenshot, report e verifiche

Elenco anomalie	Criticità riscontrate e relative azioni
Verbale o esito di validazione	Conferma del soddisfacimento dei criteri di validazione e accettazione del servizio ripristinato

La documentazione prodotta deve essere conservata secondo le modalità previste dal sistema documentale della Regione Piemonte.

11. TEST ED ESERCITAZIONI

Le attività di test rappresentano uno degli elementi fondamentali del sistema di Disaster Recovery della Regione Piemonte e consentono di verificare periodicamente l'efficacia delle strategie adottate, l'adeguatezza delle procedure operative e la capacità delle strutture coinvolte di eseguire correttamente le attività di recovery.

I test hanno inoltre lo scopo di individuare eventuali criticità, verificare il raggiungimento degli obiettivi di recovery, raccogliere evidenze documentali e attivare processi di miglioramento continuo.

11.1. Walkthrough documentale

Il Walkthrough consiste nella revisione strutturata del Piano e della documentazione correlata da parte dei soggetti coinvolti.

L'attività è finalizzata a verificare:

- completezza della documentazione;
- aggiornamento di ruoli e contatti;
- coerenza con gli altri piani;
- adeguatezza delle procedure.

11.2. Tabletop Exercise

Il Tabletop Exercise consiste nella simulazione guidata di uno scenario di Disaster Recovery.

I partecipanti analizzano lo scenario ipotizzato verificando:

- processi decisionali;
- correttezza delle escalation;
- coordinamento tra strutture;
- efficacia delle comunicazioni;
- applicabilità delle procedure di recovery.

11.3. Test tecnico selettivo

Il test tecnico selettivo è finalizzato alla verifica di specifiche componenti tecnologiche.

Può riguardare:

- sistemi di backup;

- soluzioni di replica;
- basi dati;
- infrastrutture virtuali;
- sistemi di autenticazione;
- apparati di rete;
- servizi cloud.

L'obiettivo è verificare la corretta esecuzione delle procedure e l'effettiva recuperabilità degli elementi testati.

11.4. Simulazione operativa di Disaster Recovery

La simulazione operativa prevede l'attivazione controllata delle procedure di Disaster Recovery in condizioni quanto più possibile vicine a uno scenario reale.

La simulazione consente di verificare:

- tempi di risposta;
- correttezza delle procedure;
- coordinamento tra i team;
- raggiungimento degli obiettivi RTO;
- raggiungimento degli obiettivi RPO.

11.5. Test integrato PCO - PdGC - DRP

Il test integrato rappresenta il livello più elevato di verifica del sistema di resilienza della Regione Piemonte.

L'esercitazione coinvolge contemporaneamente:

- Piano di Continuità Operativa;
- Piano di Gestione delle Crisi;
- Piano di Disaster Recovery.

L'obiettivo è verificare il coordinamento tra governance, continuità operativa e ripristino tecnologico. Ove applicabile, i test integrati possono coinvolgere anche i fornitori strategici e altre dipendenze esterne rilevanti.

11.6. Programmazione dei test e delle esercitazioni

I test e le esercitazioni di Disaster Recovery sono pianificati nell'ambito del programma unitario di verifica del sistema di continuità e resilienza dell'Ente, coordinato con il Piano di Continuità Operativa e, ove applicabile, con il Piano di Gestione delle Crisi.
La tipologia, il perimetro e la periodicità delle prove sono definiti in funzione della criticità dei servizi, delle risultanze della valutazione del rischio, delle modifiche intervenute e degli esiti delle precedenti verifiche, evitando la duplicazione di attività equivalenti previste dai diversi piani.
La pianificazione, l'esecuzione e la registrazione degli esiti dei test e delle esercitazioni sono gestite secondo quanto previsto dal REGP_PR01 – Procedure per la sicurezza informatica. I riferimenti alle verifiche effettuate

sui singoli sistemi e servizi possono essere mantenuti nel REGP_REG04 – Perimetro di continuità operativa e ripristino.

11.7. Gestione delle evidenze

Per ogni attività di test devono essere raccolte e conservate evidenze documentali adeguate.

La documentazione deve comprendere almeno:

- scenario di prova;
- obiettivi del test;
- partecipanti coinvolti;
- risultati ottenuti;
- criticità rilevate;
- azioni correttive individuate.

I risultati costituiscono input per le attività di riesame e miglioramento continuo del Piano. Report, verbali, log e ulteriori evidenze sono mantenuti nei sistemi o nei repository individuati dall'Ente o dai soggetti gestori secondo quanto previsto dal REGP_PR01, senza duplicazione nel presente Piano.

11.8. Formazione e addestramento

La formazione del personale in materia di cybersicurezza è disciplinata dal Piano di Formazione dell'Ente. Per il personale coinvolto nelle attività di Disaster Recovery sono inoltre previste, ove necessarie, specifiche attività di addestramento sulle procedure e sugli strumenti di recovery, anche mediante i test e le esercitazioni previsti dal presente Piano.

Le relative evidenze sono gestite secondo i presidi documentali previsti per la formazione e per le esercitazioni.

12. TRACCIABILITÀ ED AUDIT

La tracciabilità delle attività rappresenta un requisito fondamentale del sistema di Disaster Recovery della Regione Piemonte e consente di dimostrare l'efficacia delle misure adottate, il rispetto delle procedure previste e la conformità agli obblighi normativi applicabili.

Ogni attività svolta nell'ambito del Disaster Recovery deve essere registrata, documentata e conservata in modo tale da consentirne la successiva verifica.

Ai fini di audit e verifiche, le evidenze sono organizzate in tre categorie: evidenze di governance, evidenze operative ed evidenze di test. Le evidenze di governance dimostrano approvazione, riesame, supervisione e stato delle azioni correttive; le evidenze operative documentano l'esecuzione delle attività di recovery; le evidenze di test attestano l'efficacia periodica delle strategie e delle procedure.

Categoria evidenza	Esempi	Finalità
Governance	Approvazione del Piano, report sintetici agli organi, verbali	Dimostrare indirizzo, supervisione e

	di riesame, stato azioni correttive	controllo
Operative	Registro attività, log, checklist, report tecnici	Dimostrare l'esecuzione controllata delle attività di recovery
Test ed esercitazioni	Scenari, risultati, scostamenti, lesson learned, piano azioni correttive	Dimostrare verifica periodica, miglioramento e tenuta del Piano

Le evidenze prodotte nell'ambito delle attività di Disaster Recovery sono mantenute nei sistemi e nei repository individuati per il relativo processo, anche presso CSI Piemonte o gli ulteriori soggetti gestori ove le attività siano da questi eseguite, purché ne siano assicurate reperibilità, riconducibilità all'evento, protezione e disponibilità ai soggetti autorizzati.

12.1. Obiettivi della tracciabilità

Il sistema di registrazione delle attività è finalizzato a:

- documentare le decisioni assunte;
- ricostruire la sequenza degli eventi;
- dimostrare il rispetto delle procedure;
- supportare audit e verifiche ispettive;
- agevolare le attività di lesson learned;
- contribuire al miglioramento continuo.

12.2. Evidenze da conservare

Le evidenze di cui al presente paragrafo si riferiscono alle attivazioni effettive del DRP; per test ed esercitazioni si applicano le regole previste nel capitolo 11.

Per ogni attivazione del DRP devono essere raccolte e conservate almeno le seguenti evidenze.

Evidenza	Descrizione
Registro attività	Cronologia delle operazioni svolte
Verbali operativi	Decisioni e coordinamento
Report tecnici	Stato avanzamento recovery
Log di sistema	Evidenze tecniche
Esiti delle verifiche di validazione	Risultati delle verifiche tecniche, applicative, sui dati e di integrazione eseguite durante il ripristino
Comunicazioni	Messaggi e notifiche rilevanti
Validazioni finali	Accettazione del ripristino
Report conclusivo	Chiusura del ripristino

12.3. Conservazione delle evidenze

Le evidenze prodotte durante le attività di Disaster Recovery sono conservate secondo le modalità e nelle fonti previste dal REGP_PR01 – Procedure per la sicurezza informatica e dagli strumenti operativi applicabili.

Le evidenze devono essere:

- accessibili ai soggetti autorizzati;
- protette da modifiche non autorizzate;
- correttamente classificate;
- disponibili per audit e verifiche.

13. MANUTENZIONE DEL PIANO

Il presente Piano di Ripristino in caso di Disastro è soggetto a riesame periodico al fine di garantirne la costante adeguatezza rispetto all'evoluzione del contesto organizzativo, tecnologico, normativo e dei servizi digitali della Regione Piemonte.

La manutenzione del Piano costituisce parte integrante del sistema di resilienza della Regione Piemonte e ha lo scopo di assicurare che le strategie e i contenuti del Piano mantengano nel tempo la loro efficacia e applicabilità, in coerenza con le procedure e le fonti informative collegate.

Le attività di manutenzione comprendono:

- verifica periodica della documentazione;
- aggiornamento delle procedure operative;
- aggiornamento di ruoli e responsabilità;
- aggiornamento delle dipendenze critiche;
- aggiornamento delle informazioni relative a sistemi e servizi rilevanti;
- aggiornamento dei riferimenti ai fornitori coinvolti nelle attività di ripristino;
- recepimento delle modifiche organizzative, infrastrutturali o normative intervenute.

Il processo di manutenzione deve essere coordinato con gli analoghi processi previsti per il Piano di Continuità Operativa e per il Piano di Gestione delle Crisi, al fine di garantire la coerenza complessiva del sistema documentale della Regione Piemonte.

13.1. Riesame ordinario

Il presente Piano è riesaminato e, ove opportuno, aggiornato periodicamente e comunque **almeno ogni due anni**, nonché nei casi che determinano il riesame straordinario di cui al paragrafo 13.2.

L'attività di riesame ha lo scopo di verificare:

- adeguatezza del modello di Disaster Recovery;
- efficacia delle strategie di ripristino adottate;
- aggiornamento delle procedure operative;
- correttezza delle informazioni riportate;
- coerenza con il Piano di Continuità Operativa;
- coerenza con il Piano di Gestione delle Crisi;
- allineamento rispetto ai requisiti normativi applicabili.

Il riesame deve essere formalizzato mediante evidenze documentali che attestino l'esecuzione delle verifiche effettuate, le eventuali modifiche approvate e le azioni da intraprendere.

13.2. Riesame straordinario

Il Piano deve essere riesaminato ogniqualvolta si verifichino condizioni che possano incidere significativamente sulla validità dei suoi contenuti o sull'efficacia delle strategie di recovery previste. L'aggiornamento del REGP_REG04, del REGP_PR01, dei runbook o delle ulteriori fonti operative non comporta di per sé la revisione del Piano qualora non incida su finalità, ambito, strategie, responsabilità, priorità o criteri di attivazione e ripristino.

In particolare, il riesame straordinario deve essere valutato in presenza di:

- attivazione reale del Piano di Disaster Recovery;
- incidenti significativi che abbiano interessato servizi rilevanti;
- risultati di test ed esercitazioni che evidenzino carenze o criticità;
- modifiche organizzative rilevanti;
- introduzione di nuovi servizi strategici o critici;
- modifiche significative dell'architettura tecnologica;
- variazioni dei livelli di servizio o degli obiettivi di recovery;
- modifiche delle dipendenze critiche;
- sostituzione di infrastrutture tecnologiche;
- introduzione di nuovi fornitori rilevanti;
- modifiche normative o regolamentari;
- rilievi derivanti da audit interni o verifiche ispettive.

Qualora il riesame evidenzi la necessità di aggiornamenti sostanziali, il Piano deve essere revisionato e sottoposto ai previsti processi di approvazione.

13.3. Gestione delle modifiche

Ogni modifica apportata al presente Piano deve essere:

- formalmente registrata;
- sottoposta a controllo documentale;
- tracciata nello storico delle revisioni;
- comunicata ai soggetti coinvolti;
- recepita negli allegati interessati.

Tipo modifica	Necessità di approvazione
Modifica sostanziale del Piano	Revisione e approvazione secondo l'iter previsto
Aggiornamento del REGP_REG04 o delle procedure operative senza impatto sui contenuti sostanziali del Piano	Non comporta di per sé la revisione del Piano
Aggiornamento di runbook, istruzioni tecniche, contatti o ulteriori dati operativi	Gestione secondo la fonte competente

La gestione delle modifiche deve garantire la possibilità di ricostruire nel tempo l'evoluzione del documento e delle strategie di Disaster Recovery adottate dalla Regione Piemonte.

13.4. Miglioramento continuo

Il miglioramento continuo costituisce uno degli elementi fondamentali del sistema di Disaster Recovery della Regione Piemonte.

Le attività di miglioramento devono essere alimentate attraverso:

- attivazioni reali del Piano;
- esercitazioni;
- test periodici;
- audit;
- verifiche ispettive;
- analisi post-evento;
- lesson learned;
- analisi delle anomalie riscontrate;
- feedback dei soggetti coinvolti.

Per ciascuna opportunità di miglioramento individuata devono essere definiti:

- descrizione dell'intervento;
- responsabile;
- priorità;
- tempistica di attuazione;
- modalità di verifica del completamento.

Le azioni correttive e di miglioramento devono essere monitorate fino alla loro completa attuazione e costituiscono input per i successivi riesami del Piano.

14. KPI DEL DISASTER RECOVERY

La Regione Piemonte definisce specifici indicatori di prestazione finalizzati a monitorare l'efficacia del proprio sistema di Disaster Recovery e a supportare le attività di riesame, audit e miglioramento continuo.

Gli indicatori consentono di verificare nel tempo il livello di preparazione dell'organizzazione, l'affidabilità delle strategie adottate e la capacità della Regione Piemonte di raggiungere gli obiettivi di ripristino definiti per i servizi rilevanti.

Gli indicatori riportati costituiscono un set minimo di riferimento e potranno essere adattati dall’Ente sulla base dell’effettiva disponibilità di dati e strumenti di misurazione.

14.1. Obiettivi del monitoraggio

Le attività di monitoraggio hanno lo scopo di:

- verificare l'efficacia delle misure di Disaster Recovery;
- valutare il raggiungimento degli obiettivi di ripristino;
- monitorare l'esecuzione delle esercitazioni;
- identificare aree di miglioramento;
- supportare i processi decisionali;
- fornire evidenze oggettive durante audit e verifiche.

14.2. Indicatori di prestazione

KPI	Descrizione	Frequenza	Obiettivo
Recovery entro RTO	Percentuale di recovery completati entro il tempo previsto	Annuale	>90%
Recovery entro RPO	Percentuale di recovery che rispettano il livello massimo di perdita dati ammesso	Annuale	>90%
Test DR eseguiti	Numero di test effettuati rispetto al programma previsto	Annuale	≥90%
Test con esito positivo	Test completati con tutti i passi previsti, senza rollback e con sole eventuali non conformità minori non bloccanti.	Annuale	≥90%
Azioni correttive chiuse	Percentuale di azioni di miglioramento completate	Semestrale	>90%
Copertura sistemi	Copertura dei sistemi sottoposti a test negli ultimi 12 mesi	Annuale	100%

Gli indicatori sono riesaminati periodicamente nell'ambito delle attività di riesame del Piano e possono essere aggiornati in funzione dell'evoluzione del contesto organizzativo e tecnologico.

14.3. Analisi dei risultati

I risultati degli indicatori devono essere analizzati periodicamente al fine di individuare:

- eventuali tendenze negative;
- ritardi nell'attuazione delle misure;
- criticità ricorrenti;
- necessità di aggiornamento delle strategie di recovery;
- opportunità di miglioramento.

L'analisi dei KPI costituisce un elemento di supporto per i riesami periodici e per l'aggiornamento del Piano.

14.4. Reporting direzionale

I risultati significativi sono portati all'attenzione degli organi amministrativi e direttivi competenti in forma aggregata e proporzionata al livello di governance.

14.5. Gestione delle non conformità e delle azioni correttive

Le anomalie, le non conformità e gli scostamenti rilevati durante attivazioni reali, test, esercitazioni, audit o riesami devono essere registrati e gestiti tramite un piano di azioni correttive.

La reportistica deve evidenziare:

- andamento degli indicatori;
- obiettivi raggiunti;
- scostamenti rilevati;
- azioni correttive attivate;
- priorità di miglioramento.

Le informazioni raccolte costituiscono evidenza documentale delle attività di monitoraggio e supportano le verifiche di conformità rispetto ai requisiti previsti dalla normativa NIS2 e dalle disposizioni ACN.

15. RACCORDI OPERATIVI E FONTI INFORMATIVE

Il presente Piano utilizza le fonti informative, procedurali e tecniche previste dall'impianto documentale della Regione Piemonte, evitando la creazione o la duplicazione di allegati specifici quando le medesime informazioni sono già mantenute in altre fonti.

In particolare:

- il REGP_REG04 – Perimetro di continuità operativa e ripristino mantiene il perimetro dei sistemi e servizi, i relativi parametri di continuità e ripristino, le priorità, le principali dipendenze, le strategie applicabili e i riferimenti alla documentazione tecnica;
- il REGP_PR01 – Procedure per la sicurezza informatica disciplina le modalità procedurali comuni per l'attivazione e la gestione delle attività di ripristino, le registrazioni, le comunicazioni, la validazione e la gestione dei test e delle relative evidenze;
- i nominativi e i recapiti relativi ai ruoli di sicurezza informatica sono mantenuti nella fonte nominativa vigente individuata dall'Ente;
- i contatti operativi, gli obblighi, i livelli di servizio e le modalità di escalation dei fornitori sono mantenuti nelle fonti contrattuali e operative applicabili;
- i runbook, le checklist, le configurazioni e le istruzioni tecniche relative ai singoli sistemi e servizi sono mantenuti dalle strutture competenti, da CSI Piemonte o dagli ulteriori soggetti gestori e sono richiamati senza duplicarne il contenuto;
- registri, ticket, log, report, verbali, esiti di validazione e ulteriori evidenze prodotte durante recovery, test ed esercitazioni sono mantenuti nei sistemi e nei repository utilizzati per il relativo processo.

L'aggiornamento di tali fonti non comporta di per sé la revisione del presente Piano, salvo che la modifica incida sugli elementi sostanziali da esso disciplinati.

PIANO DI GESTIONE DELLE CRISI

Verifiche ed approvazioni

ver.	redazione		controllo ed approvazione		autorizzazione all'emissione	
	nome	data	nome	data	nome	data
v01						

Stato delle variazioni

ver.	paragrafo o pagina	descrizione della variazione
v01	Tutto il documento	Prima versione del documento

SOMMARIO

INDICE DELLE ABBREVIAZIONI....3
PREMESSA....4
1. FINALITÀ E AMBITO DI APPLICAZIONE....4
1.1. Finalità....4
1.2. Ambito....5
1.3. Relazione con il sistema documentale....5
1.4. Tracciabilità con ACN ID.IM-04....5
2. DEFINIZIONE DI CRISI....6
2.1. Criteri....7
3. MODELLO DI GESTIONE DELLA CRISI....7
3.1. Processo di gestione della crisi....8
4. ORGANIZZAZIONE E RUOLI....8
4.1. Struttura di gestione della crisi....8
4.2. Matrice RACI....9
5. ATTIVAZIONE DELLA CRISI....10
5.1. Condizioni di attivazione....10
5.2. Processo di attivazione....10
5.3. Processo....11
6. PROCESSO DECISIONALE....11
7. COMUNICAZIONE DI CRISI....12
7.1. Livelli di comunicazione....12
8. RACCORDO CON PCO E DRP....12
9. RACCORDO CON GLI ADEMPIMENTI E LE NOTIFICHE NIS....12
10. CHIUSURA DELLA CRISI....13
11. LESSON LEARNED E MIGLIORAMENTO....14
12. TEST ED ESERCITAZIONI....15
12.1. Walkthrough documentale....16
12.2. Tabletop Exercise....16
12.3. Simulazione di crisi....16
12.4. Test integrato PdGC-PCO-DRP....16
12.5. Programmazione delle esercitazioni....17
12.6. Gestione delle evidenze....17
12.7. Formazione....18
13. MANUTENZIONE DEL PIANO....18
13.1. Riesame ordinario....18

13.2. Riesame straordinario....19
13.3. Gestione delle modifiche....19
13.4. Miglioramento continuo....19
14. KPI....20
14.1. Obiettivi del monitoraggio....20
14.2. Indicatori di prestazione....20
14.3. Analisi dei risultati....20
14.4. Reporting direzionale....20
14.5. Gestione delle azioni correttive....21
15. RACCORDI OPERATIVI E FONTI INFORMATIVE....21

INDICE DELLE ABBREVIAZIONI

ACN	*Agenzia per la Cybersicurezza Nazionale*
BCP	*Business Continuity Plan*
BIA	*Business Impact Analysis*
CISO	*Chief Information Security Officer*
CIO	*Chief Information Officer*
CSIRT	*Computer Security Incident Response Team*
DR	*Disaster Recovery*
ICT	*Information and Communication Technology*
ID.IM	*Identify - Incident Management*
IRT	*Incident Response Team*
NIS2	*Direttiva (UE) 2022/2555 sulla cybersicurezza*
RPO	*Recovery Point Objective*
RTO	*Recovery Time Objective*
MTPD	*Maximum Tolerable Period of Disruption*
SIEM	*Security Information and Event Management*
SLA	*Service Level Agreement*
SOC	*Security Operations Center*

PREMESSA

Il presente **Piano di Gestione delle Crisi** (**PdGC**) costituisce il documento di indirizzo e pianificazione strategica adottato dalla Regione Piemonte per la governance delle situazioni di crisi che possono incidere sui sistemi informativi e di rete rilevanti, sulla continuità dei servizi digitali o sul corretto esercizio delle funzioni istituzionali della Regione Piemonte. Il Piano è sottoposto all'approvazione degli organi di amministrazione e direttivi competenti, in coerenza con il quadro normativo NIS e con la misura ACN ID.IM-04.
La gestione della crisi prevede l'attivazione di un **assetto temporaneo di coordinamento**, costituito dal Comitato di Crisi, quale sede collegiale di valutazione, indirizzo e coordinamento, e dalla funzione di Crisis Manager, incaricata del coordinamento operativo complessivo delle attività.
Tale assetto opera nel rispetto dell'organizzazione e delle competenze definite dagli atti vigenti della Regione Piemonte e dal REGP_POL01 - Organizzazione per la Sicurezza Informatica e non introduce autonomamente nuovi ruoli organizzativi permanenti né modifica le responsabilità formalmente attribuite alle strutture regionali.
La funzione di Crisis Manager è svolta dal Direttore della Direzione competente per materia in relazione al servizio o alla funzione istituzionale prevalentemente interessata dall'evento. Il Comitato di Crisi è costituito dal medesimo Direttore, dal responsabile del servizio interessato e dal Settore A1911A - Sistema informativo regionale per i profili di cybersicurezza. In relazione alla natura e all'estensione dell'evento possono essere coinvolte, a supporto del Comitato, ulteriori strutture regionali o soggetti esterni competenti.
I nominativi, i recapiti e le eventuali sostituzioni delle figure individuate in base alle funzioni organizzative previste dal presente Piano sono mantenuti nelle fonti organizzative e operative vigenti dell'Ente. Il loro aggiornamento non comporta revisione del Piano qualora non modifichi il modello di governance, le responsabilità o i criteri decisionali qui definiti.

1. FINALITÀ E AMBITO DI APPLICAZIONE

1.1. Finalità

Il Piano di Gestione delle Crisi ha la finalità di:

- definire il modello organizzativo per la gestione delle crisi;
- assicurare l'assunzione tempestiva delle decisioni necessarie alla tutela della continuità dei servizi e delle attività istituzionali;
- garantire il coordinamento delle strutture coinvolte nella gestione degli eventi di crisi;
- disciplinare i flussi informativi e le comunicazioni interne ed esterne;
- assicurare il rispetto degli obblighi normativi e regolamentari, inclusi quelli derivanti dalla normativa NIS2;
- definire criteri, responsabilità e modalità di costituzione e funzionamento del Comitato di Crisi;
- definire il ruolo e le responsabilità della funzione di Crisis Manager e il relativo criterio di attribuzione nell'ambito dell'assetto organizzativo regionale;
- assicurare il raccordo tra gestione ordinaria degli incidenti, continuità operativa, ripristino tecnologico e governance della crisi;
- supportare il miglioramento continuo delle capacità di resilienza della Regione Piemonte.

Il Piano disciplina esclusivamente gli aspetti di governance, coordinamento, comunicazione e processo decisionale della gestione delle crisi. Le attività operative di gestione degli incidenti, continuità operativa e ripristino tecnologico sono disciplinate rispettivamente dal Piano di Gestione degli Incidenti, dal Piano di Continuità Operativa e dal Piano di Ripristino in caso di Disastro.

1.2. Ambito

Il Piano si applica agli eventi che richiedono il coinvolgimento delle strutture di coordinamento amministrativo e strategico della Regione Piemonte, qualora tali eventi non possano essere gestiti esclusivamente tramite i processi ordinari di Incident Management.

Il PdGC può essere attivato indipendentemente dall'attivazione del PCO o del DRP qualora la natura dell'evento richieda decisioni straordinarie, coordinamento interdirezionale, comunicazioni istituzionali o gestione di impatti normativi e reputazionali. Analogamente, il PCO e il DRP possono essere attivati senza dichiarazione dello stato di crisi quando l'evento rimane gestibile nell'ambito dei rispettivi processi operativi.

Sono compresi:

- sistemi informativi e di rete rilevanti ai sensi della normativa NIS2;
- servizi per i quali sono state effettuate le analisi di BIA e risk assessment.

1.3. Relazione con il sistema documentale

Documento	Finalità
Business Impact Analysis	Identificazione servizi rilevanti
Risk Assessment	Valutazione rischi
Piano per la gestione degli incidenti di sicurezza informatica	Gestione operativa eventi
REGP_PIA07 - Piano Continuità Operativa	Definizione strategie
REGP_PIA09 - Piano Gestione delle Crisi (presente documento)	Governance della crisi
REGP_PIA08 - Piano di ripristino in caso di Disastro (DRP)	Ripristino tecnico
REGP_POL01 - Organizzazione per la Sicurezza Informatica	Assetto organizzativo, ruoli, responsabilità e canali di comunicazione in materia di cybersicurezza
REGP_PR01 - Procedure per la Sicurezza Informatica	Modalità operative comuni per l'attuazione dei processi e dei piani di sicurezza informatica
REGP_REG04 – Perimetro di continuità operativa e ripristino	Perimetro dei sistemi e servizi, parametri di continuità e ripristino, priorità e principali dipendenze

1.4. Tracciabilità con ACN ID.IM-04

Il presente Piano assicura la copertura dei contenuti richiesti dalla misura ACN ID.IM-04 per il Piano di Gestione delle Crisi secondo la seguente corrispondenza:

Requisito	Copertura documentale
Ruoli e responsabilità in situazione di crisi	Cap. 4; REGP_POL01 e fonte nominativa vigente dell'Ente
Procedure da seguire in situazione di crisi	Capp. 3, 5, 6 e 10; REGP_PR01 – Procedure per la sicurezza informatica
Modalità di comunicazione tra i soggetti coinvolti e con le autorità competenti	Cap. 7; REGP_POL01; Piano di Gestione degli Incidenti e Procedure per la Sicurezza Informatica, per quanto di rispettiva competenza
Approvazione, riesame e aggiornamento del Piano	Frontespizio e Cap. 13

Per l'assetto organizzativo generale e per le attribuzioni dei ruoli di cybersicurezza si applica il **REGP_POL01 - Organizzazione per la Sicurezza Informatica**, senza duplicazione nel presente Piano.

2. DEFINIZIONE DI CRISI

Una crisi è un evento che, per gravità, durata o ampiezza degli impatti, richiede il coinvolgimento delle strutture di coordinamento strategico e amministrativo della Regione Piemonte e l'adozione di processi decisionali straordinari.

La valutazione della severità dell'evento tiene conto dei risultati delle attività di classificazione dei servizi, Business Impact Analysis e Risk Assessment. Sono considerati in particolare la criticità dei servizi coinvolti, le dipendenze critiche interessate, la rilevanza delle funzioni istituzionali supportate e gli obblighi normativi applicabili.

Livello	Descrizione	Gestione prevalente	Governance applicabile
0	Incidente	Processi ordinari di Incident Management	Strutture operative competenti
1	Emergenza	Attivazione delle misure di continuità o recovery circoscritte	Strutture tecniche e organizzative competenti secondo PCO e/o DRP
2	Grave interruzione	PCO e/o DRP, monitoraggio rafforzato ed escalation	organi di amministrazione e direttivi competenti informati, ove necessario; valutazione dell'attivazione del PdGC
3	Crisi maggiore	Attivazione PdGC, con eventuale PCO e DRP	Comitato di Crisi e Crisis Manager

La classificazione degli eventi è effettuata considerando congiuntamente le dimensioni di impatto adottate dalla Regione Piemonte nell'ambito del processo di valutazione del rischio: impatto economico, compliance, reputazionale, livello di servizio e sicurezza del dato e delle informazioni, quest'ultima considerata nei profili di integrità, disponibilità e riservatezza.
Ai fini della gestione della crisi, la valutazione degli impatti è integrata con i fattori dinamici che possono determinare la necessità di escalation, quali la durata dell'evento, la sua estensione, l'utenza o il territorio interessati, le dipendenze coinvolte e la necessità di attivare forme straordinarie di coordinamento e decisione.
Nessuna singola dimensione di impatto o fattore di escalation determina automaticamente il livello di crisi, che deriva da una valutazione complessiva dell'evento.

L'obiettivo della classificazione è garantire che gli eventi siano gestiti con modalità proporzionate alla loro severità, evitando sia l'attivazione tardiva dei processi di crisi sia l'impiego non necessario di risorse straordinarie.
La valutazione è effettuata dalle strutture tecniche e organizzative competenti in relazione alla natura dell'evento e ai servizi interessati. Per gli eventi di natura cyber concorrono, secondo le rispettive competenze, le strutture individuate dal REGP_POL01 e dal Piano di Gestione degli Incidenti; il Punto di contatto NIS2 e il Referente CSIRT intervengono esclusivamente per gli ambiti loro attribuiti.

Il superamento di un singolo parametro, incluso l'RTO, non determina automaticamente la dichiarazione della crisi. La classificazione deriva da una valutazione complessiva degli impatti, dell'estensione, della durata, delle dipendenze coinvolte, degli obblighi normativi e della necessità di adottare decisioni straordinarie.

2.1. **Criteri**

La classificazione degli eventi è effettuata considerando congiuntamente gli impatti operativi, organizzativi, normativi, reputazionali e tecnologici. Nessun criterio è valutato in modo isolato ma nell'ambito di una valutazione complessiva finalizzata a determinare il livello di governance necessario per la gestione dell'evento.

Criterio	Descrizione	Esempi di valutazione
Economico	Conseguenze economiche dirette o indirette derivanti dall'evento	Costi straordinari, perdite economiche, necessità di interventi urgenti
Compliance	Conseguenze rispetto a obblighi normativi, regolamentari, amministrativi o contrattuali	Violazioni, obblighi di comunicazione o notifica, mancato rispetto di termini o adempimenti
Reputazionale	Conseguenze sull'immagine e sull'affidabilità istituzionale della Regione Piemonte	Rilevanza pubblica dell'evento, impatto sugli stakeholder, esposizione mediatica
Livello di servizio	Effetti sulla capacità di assicurare servizi e funzioni istituzionali	Interruzione o degrado dei servizi, indisponibilità di funzioni rilevanti
Sicurezza del dato e delle informazioni	Compromissione dell'integrità, disponibilità o riservatezza delle informazioni	Alterazione, indisponibilità, perdita, divulgazione o accesso non autorizzato a dati e informazioni
Estensione	Ampiezza dell'evento e numero di strutture, sistemi, servizi o territori interessati	Coinvolgimento di più servizi, Direzioni o ambiti territoriali
Durata	Durata effettiva o prevista degli effetti dell'evento	Prolungamento del disservizio, superamento dei parametri di continuità o ripristino applicabili
Utenza interessata	Ampiezza e rilevanza dei soggetti interessati dall'evento	Cittadini, imprese, enti, personale regionale o altre categorie di utenti
Dipendenze coinvolte	Propagazione degli effetti attraverso dipendenze organizzative, tecnologiche o di fornitura	Coinvolgimento di altri servizi, infrastrutture o fornitori rilevanti
Necessità di coordinamento straordinario	Necessità di decisioni o raccordi che eccedono la gestione ordinaria dell'evento	Coinvolgimento di più strutture, decisioni straordinarie, comunicazioni istituzionali rilevanti

3. **MODELLO DI GESTIONE DELLA CRISI**

La gestione della crisi adottata dalla Regione Piemonte si basa su un modello integrato che consente di individuare tempestivamente gli eventi rilevanti, valutarne gli impatti, attivare i livelli di governance appropriati e coordinare le attività necessarie al contenimento degli effetti e al ripristino delle condizioni operative.
Il modello distingue chiaramente:

- le attività di rilevazione, registrazione e gestione ordinaria degli eventi e degli incidenti, disciplinate dal Piano di Gestione degli Incidenti;
- le attività di continuità operativa disciplinate dal Piano di Continuità Operativa;

- le attività di ripristino tecnologico disciplinate dal Piano di Ripristino in caso di Disastro;
- le attività di governance, coordinamento strategico, comunicazione e processo decisionale disciplinate dal presente Piano di Gestione delle Crisi.

La gestione della crisi si articola nelle fasi riportate di seguito.

Fase	Finalità
Identificazione dell'evento	Rilevazione, registrazione e prima gestione dell'evento
Valutazione e classificazione	Analisi degli impatti e determinazione del livello di severità
Escalation	Valutazione della necessità di coinvolgere la governance di crisi
Attivazione della crisi	Dichiarazione dello stato di crisi e attivazione del Comitato di Crisi
Gestione e coordinamento	Assunzione delle decisioni e coordinamento delle attività
Monitoraggio	Verifica continua dell'evoluzione dell'evento
Stabilizzazione e chiusura	Conclusione formale della crisi
Lesson learned	Analisi post evento e miglioramento continuo

I criteri di classificazione e di escalation sono definiti nel capitolo 2 del presente Piano. Le modalità operative di attivazione, coordinamento e registrazione della gestione della crisi sono disciplinate nel REGP_PR01 – Procedure per la sicurezza informatica.

3.1. Processo di gestione della crisi

Le attività di identificazione e classificazione dell'evento sono svolte nell'ambito dei processi ordinari di gestione degli incidenti.

Qualora l'evento evidenzi impatti tali da richiedere decisioni straordinarie, il coinvolgimento di più strutture organizzative, comunicazioni istituzionali rilevanti o l'attivazione coordinata di più piani di resilienza, viene avviato il processo di escalation previsto dal presente Piano.

Quando l'escalation evidenzia la possibile sussistenza delle condizioni di crisi, il Comitato di Crisi è convocato secondo le modalità operative definite nel REGP_PR01. Sulla base delle informazioni disponibili è valutata e formalizzata, secondo le competenze applicabili, l'attivazione del modello di gestione della crisi.

4. ORGANIZZAZIONE E RUOLI

4.1. Struttura di gestione della crisi

L'assetto generale dei ruoli e delle responsabilità in materia di cybersicurezza è definito dal REGP_POL01 - Organizzazione per la Sicurezza Informatica e dagli atti organizzativi vigenti della Regione Piemonte. Il presente Piano non replica tale assetto e disciplina esclusivamente la composizione della struttura temporanea di gestione della crisi, le relative funzioni e i raccordi specifici necessari durante una situazione di crisi.

La struttura temporanea è costituita dal Comitato di Crisi e dalla funzione di Crisis Manager secondo i criteri definiti nel presente paragrafo.

Comitato di Crisi

Il Comitato di Crisi costituisce la sede temporanea di coordinamento collegiale attivata in presenza delle condizioni previste dal presente Piano.

Il Comitato è costituito:

- dal Direttore della Direzione competente per materia in relazione al servizio o alla funzione istituzionale prevalentemente interessata dall'evento;

- dal responsabile del servizio interessato;
- dal Settore A1911A - Sistema informativo regionale, quale struttura competente per il raccordo sui profili di cybersicurezza.

In relazione alla natura, all'ampiezza e agli impatti dell'evento possono essere coinvolte ulteriori strutture regionali, fornitori o altri soggetti competenti, senza che tale coinvolgimento modifichi la composizione di base del Comitato.

Il Comitato:

- valuta il quadro complessivo della situazione;
- formalizza l'attivazione del modello di gestione della crisi;
- definisce le priorità e gli indirizzi necessari al coordinamento della risposta;
- valuta le misure straordinarie da adottare;
- monitora l'evoluzione della situazione;
- formalizza la chiusura della crisi.

Il Comitato opera nel rispetto delle competenze attribuite ai suoi componenti e alle strutture regionali dagli atti organizzativi vigenti. Le decisioni che richiedono specifici atti amministrativi, gestionali o di indirizzo restano in capo agli organi o alle figure competenti secondo l'ordinamento regionale.

Funzione di Crisis Manager

La funzione di Crisis Manager è svolta dal Direttore della Direzione competente per materia in relazione al servizio o alla funzione istituzionale prevalentemente interessata dall'evento. L'attribuzione della funzione deriva pertanto dalla competenza organizzativa sull'ambito interessato dalla crisi e non costituisce l'istituzione di un ulteriore ruolo organizzativo permanente.

Il Crisis Manager:

- assicura il coordinamento operativo delle attività conseguenti alle decisioni assunte dal Comitato di Crisi;
- mantiene il quadro informativo aggiornato;
- assicura il raccordo tra le strutture coinvolte e tra i piani eventualmente attivati;
- monitora l'attuazione delle decisioni;
- assicura la tracciabilità delle decisioni e delle principali attività;
- predispone gli elementi necessari alla valutazione della chiusura della crisi.

Strutture regionali competenti

Le strutture regionali interessate concorrono, per gli ambiti di rispettiva competenza, alla valutazione degli impatti, all'attuazione delle decisioni, alla gestione dei servizi coinvolti e al ritorno alle normali condizioni operative.

Per i profili specificamente attinenti alla cybersicurezza, il raccordo tecnico-organizzativo nell'ambito del Comitato di Crisi è assicurato dal Settore A1911A - Sistema informativo regionale, in coerenza con il REGP_POL01. Il Settore A1910A - Servizi infrastrutturali e tecnologici e le ulteriori strutture competenti sono coinvolti, ove necessario, in relazione alla natura dell'evento e ai sistemi o servizi interessati.

Il **Punto di contatto NIS2**, il **Referente CSIRT**, le strutture competenti in materia di comunicazione istituzionale e il **DPO/struttura privacy** intervengono, ove applicabile, esclusivamente nell'ambito delle rispettive attribuzioni definite dal REGP_POL01, dagli atti organizzativi e dalla documentazione specialistica applicabile.

4.2. Matrice RACI

La seguente matrice rappresenta esclusivamente le funzioni esercitate nell'ambito della gestione della crisi e non introduce ulteriori ruoli organizzativi permanenti rispetto a quelli definiti nel REGP_POL01. Ai fini della lettura della matrice, la colonna "Crisis Manager" rappresenta la funzione esercitata dal Direttore

competente per materia, mentre la colonna “Comitato di Crisi” rappresenta le responsabilità esercitate collegialmente dalla struttura temporanea di coordinamento. Per le attività di gestione degli incidenti, continuità operativa, Disaster Recovery, notifiche NIS, protezione dei dati personali e comunicazione istituzionale si applicano le responsabilità definite dal REGP_POL01 e dai rispettivi documenti specialistici.

Attività	Comitato di Crisi	Crisis Manager	Strutture competenti
Valutazione dell'attivazione del modello di crisi	A	R	C
Formalizzazione dell'attivazione della crisi	A	R	I
Definizione delle priorità e degli indirizzi di crisi	A	R	C
Coordinamento dell'attuazione delle decisioni	I	A/R	R
Monitoraggio dell'evoluzione della crisi	A	R	C
Proposta di chiusura	C	R	C
Formalizzazione della chiusura	A	R	I
Lesson learned e monitoraggio delle azioni conseguenti	A	R	C

Legenda: A = Accountable; R = Responsible; C = Consulted; I = Informed.
L'attribuzione delle attività operative alle singole strutture è definita in relazione alla natura dell'evento e alle competenze organizzative vigenti e può essere dettagliata nei presidi operativi del Piano.

5. ATTIVAZIONE DELLA CRISI

5.1. Condizioni di attivazione

La dichiarazione dello stato di crisi è valutata quando la gestione dell'evento richiede:

- decisioni straordinarie;
- coinvolgimento degli organi di amministrazione e direttivi competenti;
- attivazione simultanea di più piani di resilienza;
- comunicazioni istituzionali rilevanti;
- gestione di obblighi normativi significativi.

L'attivazione della crisi non coincide automaticamente con l'attivazione del Piano di Continuità Operativa o del Piano di Ripristino in caso di Disastro.
Analogamente il PCO e il DRP possono essere attivati senza dichiarazione dello stato di crisi.

5.2. Processo di attivazione

La proposta di escalation verso il modello di gestione della crisi può essere formulata dalle strutture regionali competenti in relazione alla natura dell'evento e ai servizi interessati. Per gli eventi di natura cyber, la valutazione è effettuata in raccordo con le strutture e le figure individuate dal REGP_POL01 e dal Piano di Gestione degli Incidenti.
Ricevuta la proposta di escalation, il Comitato di Crisi è convocato secondo le competenze organizzative vigenti e le modalità definite nel REGP_PR01 – Procedure per la sicurezza informatica. Il Comitato valuta il quadro disponibile e, ove ne ricorrano le condizioni, formalizza l'attivazione del modello di gestione della crisi.
L'attivazione comporta:

- formalizzazione e tracciatura della decisione;
- avvio delle registrazioni dell’evento negli strumenti applicabili;

- attivazione della funzione di Crisis Manager;
- attivazione dei flussi informativi previsti;
- coinvolgimento delle strutture competenti in relazione all'evento.

5.3. **Processo**

Le fasi del processo di gestione della crisi sono descritte nel Capitolo 3 del presente Piano.
Le modalità operative di attivazione, convocazione e costituzione della struttura temporanea di coordinamento della crisi sono disciplinate nel REGP_PR01 – Procedure per la sicurezza informatica.

6. **PROCESSO DECISIONALE**

Durante la gestione della crisi tutte le decisioni devono essere assunte secondo principi di:

- tempestività;
- proporzionalità;
- tracciabilità;
- responsabilità;
- verificabilità.

Le decisioni assunte devono essere tracciate negli strumenti utilizzati per la gestione dell'evento secondo quanto previsto dal REGP_PR01 – Procedure per la sicurezza informatica.
Per ogni decisione vengono registrati almeno:

- data e ora;
- soggetto decisionale;
- motivazione;
- azioni richieste;
- responsabile dell'attuazione;
- scadenza;
- stato di avanzamento.

Il Crisis Manager provvede al monitoraggio sistematico dell'esecuzione delle decisioni assunte dal Comitato di Crisi.

Attività	Evidenza prodotta
Analisi della situazione	Quadro aggiornato della situazione
Definizione priorità	Elenco priorità approvate
Assunzione decisioni	Registro decisioni
Assegnazione attività	Piano d'azione
Monitoraggio	Stato avanzamento attività

7. COMUNICAZIONE DI CRISI

7.1. Livelli di comunicazione

Per la predisposizione dei messaggi sono utilizzati, ove previsti, i modelli e i canali definiti nel REGP_PR01 – Procedure per la sicurezza informatica e negli ulteriori strumenti di comunicazione adottati dall'Ente.

Livello	Destinatari	Obiettivo	Documento di riferimento
Operativo	Strutture tecniche e organizzative, fornitori e soggetti coinvolti	Coordinamento operativo dell'evento	Piano per la gestione degli incidenti di sicurezza informatica, PCO e/o DRP
Direzionale	Strutture e livelli di governance competenti	Supporto decisionale e gestione della crisi	Presente Piano
Autorità NIS	Autorità nazionale competente NIS	Adempimenti e comunicazioni previsti dalla disciplina NIS	REGP_POL01 e REGP_PR01
CSIRT Italia	CSIRT Italia	Interlocuzioni e notifiche relative agli incidenti	REGP_POL01, Piano per la gestione degli incidenti di sicurezza informatica e REGP_PR01
Istituzionale esterna	Utenti, cittadini, imprese e altri stakeholder	Comunicazione pubblica e istituzionale	REGP_POL01 e presidi di comunicazione dell'Ente

Le modalità e i contenuti delle comunicazioni istituzionali esterne sono definiti dalle strutture regionali competenti in materia di comunicazione istituzionale secondo quanto previsto dal REGP_POL01. Il presente Piano disciplina il raccordo di tali comunicazioni con la gestione della crisi senza ridefinirne le responsabilità organizzative.

8. RACCORDO CON PCO E DRP

Il Piano di Gestione delle Crisi costituisce l'elemento di governance del sistema di resilienza della Regione Piemonte.
Esso opera in coordinamento con:

- Piano per la gestione degli incidenti di sicurezza informatica;
- Piano di continuità operativa;
- Piano di Ripristino in caso di Disastro.

Piano	Ambito
Piano per la gestione degli incidenti di sicurezza informatica	Rilevazione, classificazione, contenimento e gestione operativa degli eventi
Piano Continuità Operativa	Continuità dei servizi e misure organizzative
Piano di Gestione delle Crisi	Governance, coordinamento e decisioni
Piano di Ripristino in caso di Disastro	Ripristino tecnologico

La gestione della crisi può comportare l'attivazione coordinata di uno o più dei documenti sopra indicati.

9. RACCORDO CON GLI ADEMPIMENTI E LE NOTIFICHE NIS

La gestione delle notifiche e degli ulteriori adempimenti connessi agli incidenti significativi non è ridefinita dal presente Piano ed è disciplinata dal **REGP_POL01 - Organizzazione per la Sicurezza Informatica**, dal

Piano di Gestione degli Incidenti, dalle **REGP_PR01 - Procedure per la Sicurezza Informatica** e dalle disposizioni normative e attuative vigenti.
Nell'ambito di una crisi derivante da un incidente di sicurezza informatica, le strutture coinvolte assicurano la tempestiva disponibilità delle informazioni necessarie all'esecuzione degli adempimenti previsti.
Le comunicazioni verso l'Autorità nazionale competente NIS sono curate dal **Punto di contatto NIS2**, con il supporto del relativo sostituto e delle strutture regionali interessate. Le interlocuzioni con lo **CSIRT Italia** e le notifiche di incidente sono curate dal **Referente CSIRT** e dagli eventuali sostituti, secondo quanto previsto dagli atti di designazione, dal REGP_POL01 e dalle procedure applicabili.
Le evidenze delle comunicazioni e delle notifiche effettuate nell'ambito dell'evento sono correlate alle ulteriori registrazioni della crisi, senza duplicare la documentazione già mantenuta nei sistemi e negli strumenti previsti dal processo di gestione degli incidenti.

10. CHIUSURA DELLA CRISI

La chiusura della crisi rappresenta il passaggio formale dalla gestione straordinaria dell'evento al ritorno alle normali condizioni operative.
La dichiarazione di chiusura può avvenire esclusivamente quando risultano soddisfatti i criteri di stabilizzazione definiti dal presente Piano e quando le strutture coinvolte hanno confermato il completamento delle attività urgenti previste.
La chiusura della crisi non esaurisce necessariamente tutte le attività conseguenti all'evento. Eventuali azioni correttive, attività di miglioramento, revisioni documentali o iniziative di formazione possono proseguire anche successivamente alla conclusione formale della crisi.
La chiusura della crisi è formalizzata e tracciata secondo le competenze organizzative vigenti e le modalità definite nel REGP_PR01 – Procedure per la sicurezza informatica. L'evidenza della chiusura può essere costituita da verbale o da altra registrazione equivalente adottata dall'Ente.

Criterio	Descrizione
Ripristino servizi	I servizi interessati risultano nuovamente disponibili o gestiti attraverso soluzioni temporanee accettabili
Stabilizzazione	Non risultano ulteriori impatti significativi o condizioni di deterioramento
Chiusura azioni urgenti	Le attività prioritarie sono state completate
Validazione della chiusura	Il Comitato di Crisi approva formalmente la chiusura

Processo di chiusura
Prima della dichiarazione di chiusura devono essere effettuate:

- verifica dello stato dei servizi;
- verifica delle comunicazioni effettuate;
- verifica del completamento delle misure urgenti;
- raccolta delle evidenze prodotte;
- valutazione delle eventuali azioni correttive da pianificare.

Verifica	Evidenza
Stato dei servizi	Report tecnico di ripristino
Comunicazioni effettuate	Registro comunicazioni
Notifiche e obblighi normativi	Evidenze ACN e NIS2
Misure urgenti completate	Piano d'azione aggiornato
Raccolta evidenze	Fascicolo della crisi

Gli esiti delle verifiche sono presentati al Comitato di Crisi che, sulla base delle informazioni disponibili, dichiara formalmente conclusa la gestione della crisi.
La documentazione minima di chiusura comprende:

- verbale di chiusura;
- registro delle decisioni aggiornato;
- registro delle comunicazioni;
- evidenze delle notifiche effettuate;
- report finale di crisi;
- elenco delle azioni correttive e di miglioramento.

Output della chiusura
La conclusione della crisi comporta:

- archiviazione della documentazione dell'evento;

- aggiornamento delle registrazioni relative all'evento;
- avvio delle attività di lesson learned;
- identificazione delle azioni correttive e di miglioramento;
- eventuale aggiornamento del Piano di Gestione delle Crisi, del Piano di Continuità Operativa e del Piano di Ripristino in caso di Disastro.

Gli elementi raccolti costituiscono parte integrante del processo di miglioramento continuo del sistema di resilienza della Regione Piemonte.
La documentazione prodotta è conservata secondo le modalità previste dal sistema documentale della Regione Piemonte e resa disponibile per attività di audit, verifica ispettiva e riesame.

11. LESSON LEARNED E MIGLIORAMENTO

Al termine di ogni crisi significativa la Regione Piemonte effettua un'attività strutturata di analisi post-evento finalizzata a comprendere le cause dell'accaduto, valutare l'efficacia delle misure adottate e individuare eventuali opportunità di miglioramento.
Le attività di lesson learned consentono di trasformare l'esperienza acquisita durante la gestione della crisi in iniziative concrete di rafforzamento della resilienza organizzativa e digitale della Regione Piemonte.
L'analisi post-evento comprende almeno:

- raccolta e classificazione delle evidenze;
- ricostruzione cronologica degli eventi;

- analisi delle cause e dei fattori che hanno contribuito all'evento;
- valutazione dell'efficacia delle decisioni assunte;
- valutazione dell'efficacia delle comunicazioni effettuate;
- valutazione del coordinamento tra le strutture coinvolte;
- valutazione dell'efficacia dell'integrazione con il Piano di Gestione degli Incidenti, il Piano di Continuità Operativa e il Piano di Ripristino in caso di Disastro;
- identificazione di eventuali criticità organizzative, procedurali, tecnologiche o contrattuali.

L'analisi post-evento è formalizzata mediante apposita reportistica e costituisce evidenza della gestione della crisi.
Per ciascuna criticità rilevata sono individuate specifiche azioni correttive e di miglioramento, assegnando:

- un responsabile;
- una priorità;
- una data obiettivo;
- una modalità di verifica dell'efficacia dell'intervento.

Le azioni correttive e di miglioramento sono monitorate fino alla loro completa attuazione e costituiscono input per:

- aggiornamento del presente Piano;
- aggiornamento del Piano di Continuità Operativa;
- aggiornamento del Piano di Ripristino in caso di Disastro;
- aggiornamento del Piano di Gestione degli Incidenti;
- aggiornamento delle procedure organizzative correlate;
- definizione delle future attività di formazione;
- pianificazione delle esercitazioni.

I risultati delle attività di lesson learned sono condivisi con le strutture interessate e costituiscono uno degli elementi fondamentali del processo di miglioramento continuo del sistema di resilienza organizzativa e digitale della Regione Piemonte.
La reportistica e le evidenze dell'analisi post-evento sono mantenute nei sistemi e nei repository previsti dal REGP_PR01 – Procedure per la sicurezza informatica. Le azioni correttive che richiedono specifica pianificazione e monitoraggio sono ricondotte, ove applicabile, al REGP_REG03 – Registro operativo delle azioni di adeguamento.

12. TEST ED ESERCITAZIONI

Le attività di test ed esercitazione consentono di verificare periodicamente l'efficacia del modello di gestione della crisi, il livello di preparazione delle strutture coinvolte e la capacità della Regione Piemonte di assumere decisioni tempestive e coordinate in presenza di eventi rilevanti.
Le attività di verifica costituiscono inoltre uno strumento fondamentale per:

- individuare eventuali criticità;
- raccogliere evidenze oggettive;

- verificare la corretta applicazione del Piano;
- validare il coordinamento tra le strutture coinvolte;
- supportare le attività di miglioramento continuo.

12.1. Walkthrough documentale

Il Walkthrough documentale consiste nella revisione strutturata del Piano e della documentazione correlata da parte dei soggetti coinvolti nella gestione della crisi.
L'obiettivo è verificare:

- completezza della documentazione;
- correttezza delle informazioni riportate;
- aggiornamento dei ruoli e delle responsabilità;
- aggiornamento dei riferimenti documentali;
- coerenza con il Piano di Continuità Operativa;
- coerenza con il Piano di Ripristino in caso di Disastro;
- coerenza con il Piano di Gestione degli Incidenti.

12.2. Tabletop Exercise

Il Tabletop Exercise consiste nella simulazione guidata di uno scenario di crisi mediante discussione strutturata tra i partecipanti.
L'attività è finalizzata a verificare:

- processi decisionali;
- modalità di escalation;
- efficacia del coordinamento;
- correttezza dei flussi informativi;
- efficacia delle comunicazioni;
- capacità di gestione delle decisioni straordinarie.

12.3. Simulazione di crisi

La simulazione di crisi prevede la riproduzione controllata di uno scenario realistico che richiede l'attivazione delle strutture di governance della crisi.
L'attività consente di verificare:

- tempi di risposta;
- efficacia della convocazione della struttura di crisi;
- coordinamento delle strutture coinvolte;
- gestione delle comunicazioni;
- efficacia delle decisioni assunte;
- gestione degli aspetti normativi e regolamentari applicabili.

12.4. Test integrato PdGC-PCO-DRP

Il test integrato rappresenta il livello più elevato di verifica del modello di resilienza adottato dalla Regione Piemonte.
L'esercitazione coinvolge contemporaneamente:

- Piano di Gestione delle Crisi;

- Piano di Continuità Operativa;
- Piano di Ripristino in caso di Disastro.

L'obiettivo è verificare il corretto coordinamento tra:

- governance della crisi;
- continuità dei servizi;
- ripristino tecnologico;
- processo decisionale;
- gestione delle comunicazioni;
- gestione delle notifiche e degli adempimenti normativi.

Ove applicabile, i test integrati possono coinvolgere fornitori rilevanti e ulteriori soggetti esterni che contribuiscono all'erogazione dei servizi regionali.

12.5. Programmazione delle esercitazioni

La pianificazione dei test e delle esercitazioni del sistema di resilienza è gestita secondo quanto previsto dal REGP_PR01 – Procedure per la sicurezza informatica, tenendo conto:

- delle analisi di rischio;
- delle risultanze della Business Impact Analysis;
- delle lezioni apprese derivanti da crisi reali;
- delle risultanze di audit e verifiche;
- delle modifiche organizzative;
- delle modifiche tecnologiche;
- degli obiettivi di miglioramento individuati.

Le tipologie e le frequenze delle attività di verifica costituiscono valori minimi di riferimento e possono essere adeguate in funzione dell'evoluzione del contesto organizzativo, tecnologico, normativo e dei rischi rilevati.

12.6. Gestione delle evidenze

Per ogni attività di test o esercitazione devono essere raccolte e conservate evidenze adeguate.
La documentazione prodotta comprende almeno:

- scenario utilizzato;
- obiettivi dell'attività;
- partecipanti coinvolti;
- risultati ottenuti;
- eventuali criticità individuate;
- azioni correttive proposte;
- piano di miglioramento conseguente.

I risultati costituiscono input per le attività di riesame e miglioramento continuo del Piano. Report, verbali e ulteriori evidenze sono mantenuti negli strumenti individuati dall'Ente secondo quanto previsto dal REGP_PR01 – Procedure per la sicurezza informatica.

12.7. Formazione

I soggetti che, in relazione alle rispettive competenze, possono essere coinvolti nella struttura temporanea di coordinamento della crisi o nell'esercizio della funzione di coordinamento operativo devono ricevere adeguata formazione e aggiornamento, secondo quanto previsto dal Piano di formazione in materia di sicurezza informatica.
Le attività formative hanno lo scopo di:

- garantire la conoscenza dei ruoli assegnati;
- assicurare la conoscenza delle procedure previste dal Piano;
- migliorare la capacità di coordinamento;
- rafforzare la capacità di risposta agli eventi;
- favorire il corretto utilizzo degli strumenti di supporto alla gestione della crisi.

La pianificazione delle attività formative è definita nell'ambito dei programmi di formazione e sensibilizzazione adottati dalla Regione Piemonte ed è coordinata, ove applicabile, con il programma di test ed esercitazioni del sistema di resilienza.

13. MANUTENZIONE DEL PIANO

Il presente Piano è soggetto a riesame periodico al fine di garantirne la costante adeguatezza rispetto all'evoluzione del contesto organizzativo, normativo, tecnologico e dei servizi digitali della Regione Piemonte.
Le attività di manutenzione comprendono:

- verifica dell'efficacia del modello di gestione della crisi;
- verifica della coerenza con i ruoli e le responsabilità definiti nel REGP_POL01 e negli atti organizzativi vigenti;
- aggiornamento dei flussi di comunicazione;
- aggiornamento delle modalità di escalation;
- aggiornamento dei riferimenti documentali;
- aggiornamento dei collegamenti con PCO, DRP e Piano di Gestione degli Incidenti;
- recepimento delle modifiche organizzative e normative intervenute.

13.1. Riesame ordinario

Il presente Piano è riesaminato e, ove opportuno, aggiornato periodicamente e comunque **almeno ogni due anni**, nonché nei casi che determinano il riesame straordinario di cui al paragrafo 13.2.
L'attività di riesame ha lo scopo di verificare:

- adeguatezza del modello di gestione della crisi;
- efficacia delle procedure previste;
- aggiornamento della documentazione;
- coerenza con il Piano di Continuità Operativa;
- coerenza con il Piano di Ripristino in caso di Disastro;
- coerenza con il Piano di Gestione degli Incidenti;
- allineamento rispetto ai requisiti normativi applicabili.

Gli esiti del riesame devono essere formalizzati mediante adeguate evidenze documentali.

13.2. Riesame straordinario

Il Piano deve essere riesaminato anticipatamente ogniqualvolta si verifichino condizioni che possano incidere significativamente sulla validità delle informazioni contenute o sull'efficacia del modello di gestione della crisi.
Il riesame straordinario deve essere valutato almeno in presenza di:

- crisi reali;
- incidenti significativi;
- risultati di test ed esercitazioni;
- modifiche organizzative rilevanti;
- modifiche tecnologiche significative;
- modifiche normative o regolamentari;
- rilievi derivanti da audit interni;
- rilievi derivanti da verifiche ispettive;
- variazioni significative del contesto operativo.

Qualora il riesame evidenzi la necessità di aggiornamenti sostanziali, il Piano deve essere aggiornato e sottoposto ai previsti processi di approvazione.

13.3. Gestione delle modifiche

Ogni modifica apportata al presente Piano deve essere:

- formalmente registrata;
- sottoposta a controllo documentale;
- tracciata nello storico delle revisioni;
- comunicata ai soggetti interessati;
- recepita, ove necessario, nelle procedure e nelle fonti informative collegate.

Le modifiche che incidono su:

- governance;
- responsabilità;
- criteri decisionali;
- modello organizzativo;
- principi del Piano;

richiedono revisione formale del documento.
Gli aggiornamenti relativi a nominativi, contatti, sostituzioni, modalità operative, modelli, registrazioni ed evidenze sono gestiti nelle rispettive fonti competenti, tra cui la fonte nominativa vigente dell'Ente, il REGP_PR01, il REGP_REG04 e gli ulteriori strumenti operativi applicabili. Tali aggiornamenti non comportano di per sé la revisione del Piano, purché non incidano sugli elementi sostanziali di governance, responsabilità, criteri decisionali o modalità di attivazione qui definiti.

13.4. Miglioramento continuo

Crisi reali, esercitazioni, audit, verifiche ispettive, notifiche NIS2, lesson learned e monitoraggio degli indicatori costituiscono input strutturati per il miglioramento continuo del sistema di gestione delle crisi.

Le opportunità di miglioramento individuate sono registrate, assegnate a un responsabile e monitorate fino alla loro completa attuazione.
Le azioni correttive e di miglioramento costituiscono parte integrante del processo di gestione della resilienza della Regione Piemonte e sono riesaminate periodicamente nell'ambito delle attività di governance e controllo del sistema.

14. KPI

Gli indicatori riportati nel presente capitolo consentono di monitorare l'efficacia del processo di gestione delle crisi e supportano le attività di riesame, audit e miglioramento continuo.

14.1. Obiettivi del monitoraggio

Le attività di monitoraggio hanno lo scopo di:

- verificare l'efficacia del modello di gestione della crisi;
- monitorare l'esecuzione delle esercitazioni;
- verificare l'attuazione delle azioni correttive;
- valutare il rispetto degli obblighi normativi applicabili;
- individuare opportunità di miglioramento;
- supportare le attività di governance e riesame.

14.2. Indicatori di prestazione

KPI	Descrizione	Frequenza	Obiettivo
Attività di verifica svolte	Attività di test ed esercitazione completate rispetto alla pianificazione definita dalla Regione Piemonte	Annuale	Secondo programma
Azioni correttive completate	Percentuale di azioni correttive chiuse entro la data prevista	Semestrale	>90%
Notifiche effettuate nei termini	Rispetto delle tempistiche previste dalla normativa applicabile	Annuale	100%
Eventi di crisi con evidenze minime disponibili	Percentuale di crisi per le quali risultano disponibili le registrazioni e le evidenze minime previste	Annuale	100%
Lesson learned completate	Analisi post-evento formalizzate rispetto alle crisi significative gestite	Annuale	100%

14.3. Analisi dei risultati

I risultati degli indicatori devono essere analizzati periodicamente per individuare:

- eventuali tendenze negative;
- ritardi nell'attuazione delle misure correttive;
- criticità ricorrenti;
- inefficienze organizzative;
- opportunità di miglioramento.

Le risultanze costituiscono input per le attività di riesame del Piano e per gli interventi di miglioramento continuo.

14.4. Reporting direzionale

I risultati significativi degli indicatori sono condivisi con i livelli di governance competenti in forma aggregata e proporzionata alle esigenze informative della Regione Piemonte.

La reportistica può comprendere:

- andamento degli indicatori;
- obiettivi raggiunti;
- scostamenti rilevati;
- criticità emerse;
- azioni correttive avviate;
- priorità di miglioramento.

14.5. Gestione delle azioni correttive

Le anomalie, le criticità, le non conformità e gli scostamenti rilevati durante:

- crisi reali;
- esercitazioni;
- audit;
- verifiche ispettive;
- riesami periodici;

devono essere registrati e gestiti, ove richiedano specifica pianificazione e monitoraggio, attraverso il REGP_REG03 – Registro operativo delle azioni di adeguamento o gli ulteriori strumenti di pianificazione adottati dall'Ente.
Le informazioni raccolte costituiscono evidenza documentale delle attività di monitoraggio e supportano il processo di miglioramento continuo del sistema di gestione delle crisi.

15. RACCORDI OPERATIVI E FONTI INFORMATIVE

Il presente Piano utilizza le fonti organizzative, informative, procedurali e operative previste dall'impianto documentale della Regione Piemonte, evitando la creazione e la duplicazione di allegati specifici quando i relativi contenuti sono già disciplinati o mantenuti in altre fonti.
In particolare:

- il REGP_POL01 – Organizzazione per la sicurezza informatica definisce i ruoli, le responsabilità e i raccordi organizzativi di riferimento;
- la fonte nominativa vigente individuata dall'Ente mantiene i nominativi e le sostituzioni delle figure rilevanti per la sicurezza informatica;
- il REGP_PR01 – Procedure per la sicurezza informatica disciplina le modalità operative di attivazione e coordinamento della crisi, la tracciatura delle decisioni e delle comunicazioni, la gestione delle evidenze, la chiusura e le attività di analisi post-evento;
- il REGP_REG04 – Perimetro di continuità operativa e ripristino costituisce la fonte per le informazioni relative ai sistemi e ai servizi interessati, alla loro criticità, ai parametri di continuità e ripristino e alle principali dipendenze, quando rilevanti ai fini della gestione della crisi;
- il Piano per la gestione degli incidenti di sicurezza informatica disciplina la gestione degli incidenti e le relative notifiche;
- il REGP_PIA07 – Piano di continuità operativa e il REGP_PIA08 – Piano di ripristino in caso di disastro disciplinano i rispettivi processi eventualmente attivati in coordinamento con la crisi;
- i modelli e i canali per la comunicazione istituzionale sono mantenuti nelle fonti e negli strumenti adottati dalle strutture regionali competenti;

- le eventuali azioni correttive e di miglioramento sono monitorate mediante il REGP_REG03 o gli ulteriori strumenti di pianificazione applicabili;
- verbali, ticket, log, report, registrazioni e ulteriori evidenze prodotte durante la gestione della crisi sono mantenuti nei sistemi e nei repository previsti per il relativo processo.

L'aggiornamento delle predette fonti non comporta di per sé la revisione del presente Piano, salvo che la modifica incida sugli elementi sostanziali di governance, sulle responsabilità, sui criteri decisionali, sulle condizioni di attivazione o sugli ulteriori contenuti qualificanti del Piano.

ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA ADOTTATA DALLA REGIONE PIEMONTE

Approvato dall'organo di amministrazione e direttivo competente
Atto di approvazione: [indicare estremi dell'atto]
Data di approvazione: [gg/mm/aaaa]

-

INDICE

1. PREMESSA E OBIETTIVI....3

2. DOCUMENTI DI RIFERIMENTO....3

3. NORME DI RIFERIMENTO....4

4. ANALISI DEL CONTESTO DELL'ENTE....4

5. IMPIANTO ORGANIZZATIVO....5

5.1 Identificazione dei ruoli e delle responsabilità....5
5.2 Assegnazione dei ruoli e affidabilità delle persone....6
5.3 Organizzazione per la sicurezza informatica....6
5.3.1 Processi ed attività in ambito cybersicurezza....9
5.3.2 RACI - Matrice attività / ruoli /responsabilità....13
5.4 Tavoli di coordinamento....13
5.5 Canali di comunicazione....14

6. AGGIORNAMENTO....15

7. PUBBLICAZIONE....16

1. PREMESSA E OBIETTIVI

Regione Piemonte rientra nell'ambito di applicazione del decreto legislativo 4 settembre 2024, n. 138, di recepimento della direttiva (UE) 2022/2555 ("direttiva NIS2"), in quanto amministrazione regionale ricompresa nell'ambito soggettivo di applicazione del decreto. Con Determinazione del Direttore Generale dell'Agenzia per la cybersicurezza nazionale n. 136430 del 12 aprile 2025, comunicata alla Regione ai sensi dell'articolo 7, comma 3, del decreto legislativo n. 138/2024, Regione Piemonte è stata individuata quale soggetto importante ai sensi dell'articolo 6 del medesimo decreto.
L'Ente è pertanto tenuto a adottare e mantenere un assetto organizzativo, procedurale e documentale idoneo ad assicurare la gestione dei rischi per la sicurezza informatica, la prevenzione e la gestione degli incidenti, nonché il rispetto degli ulteriori obblighi previsti dalla normativa applicabile.
Il presente documento, predisposto anche ai fini del soddisfacimento del requisito GV.RR-02, punto 1, delle Linee guida NIS – Specifiche di base, fornisce una rappresentazione organica dell'assetto di sicurezza informatica della Regione Piemonte, con particolare riguardo ai ruoli, alle responsabilità e ai raccordi funzionali rilevanti ai fini della cybersicurezza dell'Ente.
Esso è redatto con finalità di descrizione dell'assetto organizzativo vigente, osservato nella prospettiva della sicurezza informatica, e costituisce quadro di riferimento per la lettura coordinata delle misure organizzative adottate o da adottare in attuazione della normativa applicabile.
Il documento non ha natura istitutiva o modificativa dell'organizzazione regionale e non sostituisce, integra o deroga ad altri atti organizzativi, ordinamentali o gestionali dell'Ente, la cui competenza permane in capo alle strutture regionali a ciò preposte secondo l'ordinamento vigente.

2. DOCUMENTI DI RIFERIMENTO

[1] – Deliberazione della Giunta regionale 3 dicembre 2024, n. 3-474, recante individuazione del Referente regionale per la cybersicurezza per la Giunta regionale e le sue strutture e istituzione del gruppo di lavoro interdirezionale per l'attuazione della normativa in materia di cybersicurezza

[2] – Determinazione dirigenziale 22 gennaio 2025, n. 11/A1000A/2025, recante istituzione del gruppo di lavoro interdirezionale "Attuazione della normativa in materia di cybersicurezza"

[3] - Deliberazione della Giunta Regionale 6 maggio 2025, n. 37-1089, "Approvazione nuova organizzazione delle Strutture dirigenziali del ruolo della Giunta Regionale"

[4] – Deliberazione della Giunta regionale 28 luglio 2025, n. 15-1430, recante disposizioni per l'adempimento degli obblighi in materia di sicurezza informatica ai sensi del decreto legislativo n. 138/2024 e, in particolare, l'individuazione dei soggetti da indicare nel Portale NIS quali organi di amministrazione e direttivi dell'Ente.

[5] – Struttura organizzativa vigente della Giunta regionale del Piemonte e declaratorie delle Direzioni e dei Settori, pubblicati sul sito istituzionale dell'Ente

[6] – Codice di comportamento dei dipendenti della Giunta della Regione Piemonte, approvato con DGR n. 1-1717 del 13/07/2015

[7] – Piano Integrato di Attività e Organizzazione (PIAO) vigente della Giunta regionale del Piemonte

[8] – Atti di nomina o designazione vigenti adottati dalla Giunta regionale e/o dalle strutture competenti in materia di cybersicurezza, ivi inclusi quelli relativi al Punto di contatto NIS2 e al relativo sostituto

[9] – Atti di designazione vigenti del Referente CSIRT e degli eventuali sostituti, adottati secondo la disciplina applicabile e l'assetto organizzativo dell'Ente.

[10] –Disciplina dell'organizzazione degli uffici regionali e disposizioni concernenti la dirigenza ed il personale: L.R. 28 luglio 2008, n. 23

[11] – REGP_POL01_ALL01 – Tabella nominativa dei ruoli di sicurezza informatica, contenente l'elenco aggiornato dei soggetti interni ed esterni aventi specifici ruoli e responsabilità in materia di sicurezza informatica e, ove pertinente, gli estremi degli atti di nomina o designazione vigenti.

3. NORME DI RIFERIMENTO

- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2).
- Decreto legislativo 4 settembre 2024, n. 138, recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.
- Legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.
- Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale, con particolare riferimento ai profili organizzativi delle pubbliche amministrazioni e al ruolo del Responsabile per la transizione digitale.
- Legge regionale 28 luglio 2008, n. 23 - Disciplina dell'organizzazione degli uffici regionali e disposizioni concernenti la dirigenza ed il personale, quale riferimento per l'assetto organizzativo della Giunta regionale e delle sue strutture.
- Determinazione ACN 127437/2026- Piattaforma, Punto di contatto e sostituto, aggiornamento delle informazioni e rappresentante NIS di cui all'articolo 7 del decreto NIS
- Determinazione ACN n. 379907/2025 - Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS, con i relativi allegati tecnici.
- Decreto del Direttore generale ACN n. 327240 del 2 settembre 2025 - Linee guida NIS - Specifiche di base - Guida alla lettura.
- Decreto del Direttore generale ACN n. 397589 del 31 dicembre 2025 - Linee guida NIS - Specifiche di base - Definizione del processo di gestione degli incidenti di sicurezza informatica.

4. ANALISI DEL CONTESTO DELL'ENTE

La Giunta regionale del Piemonte, con deliberazione n. 3-2182 del 30 gennaio 2026, ha approvato il Piano Integrato di Attività e Organizzazione (PIAO) della Giunta regionale del Piemonte per il triennio 2026-2028. Il PIAO costituisce il documento di pianificazione integrata della Giunta regionale ed è pubblicato sul sito istituzionale dell'Ente.

L'assetto organizzativo della Giunta regionale e delle sue strutture è disciplinato dalla legge regionale 28 luglio 2008, n. 23, nonché dai relativi provvedimenti organizzativi adottati ai sensi della medesima legge. In tale quadro, l'organizzazione degli uffici regionali si fonda sulla distinzione tra funzioni di indirizzo politico-amministrativo e funzioni di gestione dirigenziale, nonché sulla distribuzione delle competenze tra Direzioni e Settori.

Con riferimento ai profili rilevanti per la sicurezza informatica, il contesto organizzativo della Giunta regionale presenta un presidio specialistico centrale in materia ICT e cybersicurezza, incardinato nella Direzione A19000 - Competitività del sistema regionale.

Pertanto, per quello che riguarda il contesto organizzativo di cui al generico punto GV.OC della norma l'Ente ha documentato e individuato ogni aspetto di "missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali – che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione" tramite il PIAO.

5. IMPIANTO ORGANIZZATIVO

Il presente documento riepiloga con riferimento all'ambito della cybersicurezza:

- i ruoli e le responsabilità già definite (par. 5.1):
- i ruoli affidati in base alle competenze e all'affidabilità delle persone (par. 5.2)
- i ruoli presenti nella struttura organizzativa e nelle nomine/procure (par. 5.3)
- i tavoli di coordinamento (par. 5.4)
- i canali di comunicazione (par. 5.5)

L'impianto organizzativo è definito in conformità alla disciplina regionale sull'organizzazione degli uffici e alla normativa nazionale applicabile, nonché tenendo conto dei provvedimenti organizzativi e delle nomine formalmente adottati dall'Ente.

5.1 Identificazione dei ruoli e delle responsabilità

La Giunta regionale e le sue strutture identificano i ruoli e le responsabilità rilevanti ai fini della sicurezza informatica mediante:

- la struttura organizzativa vigente e le declaratorie delle Direzioni e dei Settori;
- i provvedimenti organizzativi attuativi della legge regionale 28 luglio 2008, n. 23;
- gli atti di conferimento degli incarichi dirigenziali e degli altri incarichi organizzativi rilevanti;
- gli atti di nomina o designazione relativi ai ruoli specialistici, inclusi quelli in materia di cybersicurezza, protezione dei dati personali e amministrazione di sistema;
- le procedure, i piani e le istruzioni operative interne che attribuiscono compiti, responsabilità e flussi di raccordo tra le strutture.

Pertanto "I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati" e sono definiti in modo da risultare coerenti con le competenze formalmente attribuite alle strutture regionali e con i requisiti organizzativi previsti dalla disciplina NIS [req. GV.RR.02].

5.2 Assegnazione dei ruoli e affidabilità delle persone

L'assegnazione dei ruoli rilevanti ai fini della sicurezza informatica avviene in coerenza con:

- le competenze richieste dal ruolo;
- l'incarico formalmente conferito;
- l'esperienza professionale e tecnica posseduta;
- i percorsi di formazione e aggiornamento attivati dall'Ente.

Per i ruoli con specifiche responsabilità in ambito cybersicurezza, l'Ente assicura l'adeguatezza delle competenze anche mediante iniziative formative dedicate e aggiornamento periodico. L'affidabilità del personale si valuta nel quadro delle regole generali applicabili al personale della Regione Piemonte, con particolare riferimento al Codice di comportamento, agli obblighi in materia di conflitto di interessi, incompatibilità e agli ulteriori adempimenti previsti dalla disciplina vigente e dagli atti interni effettivamente adottati [req. GV.RR-04, GV.PO-01.c].

5.3 Organizzazione per la sicurezza informatica

L'organizzazione per la sicurezza informatica della **Regione Piemonte** si fonda su un modello di coordinamento interdirezionale. In tale quadro, il presidio tecnico-organizzativo delle attività in materia di cybersicurezza è assicurato, nell'ambito **della Direzione A19000 - Competitività del sistema regionale**, dal **Settore A1911A - Sistema informativo regionale**, competente, tra l'altro, per la programmazione del sistema informativo regionale, l'Agenda digitale regionale e il coordinamento delle attività di digitalizzazione dei processi e dei procedimenti.
Con deliberazione della Giunta regionale 3 dicembre 2024, n. 3-474, la Regione Piemonte ha individuato il Responsabile pro tempore del Settore **A1911A - Sistema informativo regionale** quale **Referente regionale per la cybersicurezza**, per la Giunta regionale e le sue strutture. Con il medesimo provvedimento è stata altresì prevista l'istituzione di un gruppo di lavoro interdirezionale per l'attuazione della normativa in materia di cybersicurezza, successivamente istituito con determinazione dirigenziale 22 gennaio 2025, n. 11/A1000A/2025.
Riassumendo l'organizzazione dell'Ente con il punto di vista della cybersicurezza:

- Per i documenti che, in base alla disciplina NIS e alle relative specifiche di base, richiedono l'approvazione degli organi di amministrazione e direttivi, la Regione Piemonte assicura il coinvolgimento del livello direzionale competente attraverso il Comitato di coordinamento direttori, quale sede di raccordo interdirezionale prevista dall'assetto organizzativo regionale. Resta ferma la necessità che l'approvazione sia ricondotta agli organi o alle figure competenti secondo il D.Lgs. 138/2024, gli atti organizzativi dell'Ente e le eventuali deleghe formalmente adottate
- il **Settore A1911A - Sistema informativo regionale** assicura il coordinamento tecnico-organizzativo delle attività in materia di cybersicurezza, la predisposizione e l'aggiornamento della documentazione di riferimento, nonché il raccordo con le altre strutture regionali coinvolte;
- il **Referente per la cybersicurezza** coordina le attività necessarie all'attuazione della normativa in materia di cybersicurezza, promuove il monitoraggio dello stato di avanzamento degli adempimenti, assicura il coordinamento dei flussi informativi interni e il raccordo con il

Punto di contatto NIS e con il Referente CSIRT per le comunicazioni esterne di rispettiva competenza, secondo gli atti di nomina e le procedure applicabili;

- il **Gruppo di Lavoro interdirezionale** supporta l'attuazione operativa e coordinata degli obblighi in materia di cybersicurezza, favorendo il coinvolgimento delle strutture regionali competenti per i profili ICT, organizzativi, privacy, infrastrutturali, di continuità operativa e contrattuali.

L'organizzazione così definita è finalizzata ad assicurare che i documenti e i processi richiesti dalla disciplina NIS siano sviluppati e mantenuti in modo coerente, uniforme e sostenibile a livello di Ente, valorizzando il presidio specialistico centrale e il necessario coinvolgimento delle Direzioni regionali competenti.

Si riportano nel seguito i documenti che la normativa (rif. Appendice C del documento "Linee guida NIS – Specifiche di base – Guida alla lettura" - v2.0.1 - pubblicato a marzo 2026) prevede siano adottati dagli organi di amministrazione e direttivi:

Documento	Riferimento requisito[1]
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 2
Piano per la gestione degli incidenti di sicurezza informatica	RS.MA-01 punto 2

I ruoli e le responsabilità rilevanti ai fini NIS sono riepilogati nella tabella seguente, che costituisce il riferimento unitario per l'identificazione delle principali responsabilità organizzative, dei raccordi funzionali e dei processi presidiati in materia di sicurezza informatica.

I nominativi delle persone incaricate, i relativi recapiti e, ove pertinente, gli estremi degli atti di nomina o designazione sono mantenuti nella REGP_POL01_ALL01 – Tabella nominativa dei ruoli di sicurezza informatica, che costituisce fonte operativa aggiornata separatamente dal presente documento. Le variazioni dei nominativi o dei relativi atti di designazione che non comportano modifiche dei ruoli, delle responsabilità o dell'assetto organizzativo descritto nel presente documento non richiedono la revisione del REGP_POL01.

Ruoli, funzioni organizzative e responsabilità rilevanti ai fini NIS

Ruolo / funzione organizzativa	Base organizzativa / normativa	Responsabilità rilevanti ai fini NIS	Principali documenti / processi presidiati	Raccordi principali
Comitato di coordinamento direttori	art. 9, comma 4, l.r. 23/2008	sede di raccordo interdirezionale per l'esame, la condivisione e la revisione dei documenti e delle tematiche trasversali in materia di	esame e raccordo sui documenti NIS; coordinamento sugli aspetti trasversali	Direzione A19000, Settore A1911A, Direzioni regionali

1 Determinazione ACN 379907/2025, Allegato 1 - "Misure di sicurezza di base per i soggetti importanti"

Ruolo / funzione organizzativa	Base organizzativa / normativa	Responsabilità rilevanti ai fini NIS	Principali documenti / processi presidiati	Raccordi principali
		sicurezza informatica; favorisce l'allineamento tra le Direzioni, ferme restando le responsabilità attribuite agli organi di amministrazione e direttivi individuati dall'Ente ai fini della disciplina NIS		
Direzione A19000 - Competitività del sistema regionale		assicura, per quanto di competenza, il presidio direzionale sulle materie afferenti a transizione digitale, servizi ICT, cybersicurezza e attività ex art. 17 CAD	adozione degli atti di competenza; coordinamento direzionale	Comitato di coordinamento direttori, A1911A, A1910A, UTD
Settore A1911A - Sistema informativo regionale		coordinamento tecnico-organizzativo delle attività di cybersicurezza; predisposizione e aggiornamento della documentazione; raccordo con le strutture competenti	politiche e procedure di sicurezza; documentazione NIS; risk assessment e piani connessi	Referente cybersecurity, A1910A, privacy, strutture regionali
Referente per la cybersicurezza	DGR 3-474/2024	coordina l'attuazione della normativa cyber; promuove l'aggiornamento documentale; presidia i flussi informativi interni ed esterni	coordinamento adempimenti NIS; monitoraggio avanzamento; reporting	A1911A, Comitato di coordinamento direttori, Punto di contatto NIS2, GdL
Gruppo di lavoro interdirezionale cybersicurezza	DD 11/A1000A/2025	supporta l'attuazione operativa e coordinata degli obblighi in materia di cybersicurezza	supporto agli adempimenti, vulnerabilità, incidenti, misure di sicurezza	Referente cybersecurity, Direzioni regionali
Punto di contatto NIS2	art. 7 d.lgs. 138/2024; atto di designazione vigente dell'Ente	cura, secondo gli atti di designazione e la normativa applicabile, gli adempimenti verso l'autorità nazionale competente NIS, la registrazione e l'aggiornamento delle informazioni sulla piattaforma digitale NIS e il coordinamento dei flussi informativi istituzionali verso l'autorità competente	registrazione del soggetto NIS; aggiornamento delle informazioni richieste dalla normativa; raccordo sugli adempimenti verso l'autorità competente	Referente per la cybersicurezza, sostituto del punto di contatto, Referente CSIRT, strutture regionali coinvolte
Sostituto del punto di contatto NIS2	art. 7 d.lgs. 138/2024; atto di designazione vigente dell'Ente	assicura continuità operativa nelle attività del punto di contatto in caso di assenza o impedimento	supporto e sostituzione nelle comunicazioni ACN	Punto di contatto NIS2
Referente CSIRT e sostituti		interloquisce con lo CSIRT Italia e, secondo gli atti di designazione e le procedure interne, effettua le notifiche di incidente e le interlocuzioni tecniche previste dalla disciplina applicabile	processo di gestione degli incidenti; notifiche allo CSIRT Italia; relazioni e comunicazioni tecniche sugli incidenti	Punto di contatto NIS2, Referente per la cybersicurezza, Settore A1911A, strutture tecniche coinvolte
Settore competente in materia di privacy / DPO / referenti privacy di		presidiano i profili di protezione dei dati personali e il raccordo nei casi di data breach o incidenti con impatto su dati personali	data breach, valutazioni privacy collegate agli incidenti, supporto a policy e risk assessment	Referente cybersecurity, A1911A, Direzioni

Ruolo / funzione organizzativa	Base organizzativa / normativa	Responsabilità rilevanti ai fini NIS	Principali documenti / processi presidiati	Raccordi principali
Direzione				
Settore A1910A - Servizi infrastrutturali e tecnologici		presidia i profili infrastrutturali e tecnologici rilevanti per l'attuazione delle misure di sicurezza e la resilienza operativa	misure tecniche, infrastrutture, strumenti tecnologici di lavoro	A1911A, Referente cybersecurity, fornitori tecnici
RUP - Responsabile unico del progetto		assicura, per le forniture e i servizi di competenza, l'integrazione dei requisiti di sicurezza nella fase di programmazione, progettazione, affidamento ed esecuzione, con il supporto delle strutture tecniche competenti	atti di gara, capitolati, requisiti di sicurezza, clausole contrattuali	strutture richiedenti, A1911A, A1910A, DEC
DEC - Direttore dell'esecuzione del contratto, ove nominato		verifica in fase esecutiva il rispetto delle prestazioni contrattuali, inclusi gli obblighi di sicurezza e i livelli di servizio rilevanti ai fini cyber, nei casi in cui sia nominato	esecuzione del contratto, verifiche di conformità, livelli di servizio, misure di sicurezza contrattuali	RUP, strutture tecniche, fornitori
Fornitori / soggetti terzi / eventuale in house	contratto, convenzione, disciplinare, accordo di servizio	attuano le misure di sicurezza e gli obblighi contrattuali loro attribuiti; forniscono supporto tecnico-operativo nei limiti contrattuali	servizi ICT, gestione operativa, supporto specialistico, monitoraggio, manutenzione	RUP, DEC, A1911A, A1910A, Referente cybersecurity
Personale regionale e referenti di struttura		osservano le politiche di sicurezza, collaborano all'attuazione delle misure e segnalano eventi, anomalie o incidenti	attuazione operativa delle misure; segnalazioni	responsabili di struttura, A1911A, GdL

I ruoli e le responsabilità di cui alla presente tabella sono riesaminati periodicamente e, ove necessario, aggiornati in relazione a modifiche organizzative, evoluzioni normative, variazioni del perimetro NIS, incidenti significativi o mutamenti dell'esposizione ai rischi.

5.3.1 Processi ed attività in ambito cybersicurezza

I processi e le attività rilevanti ai fini della cybersicurezza della **Regione Piemonte** sono organizzati in coerenza con l'assetto organizzativo dell'Ente, con i ruoli individuati nel paragrafo 5.3 e con i documenti, i piani e le procedure adottati nelle materie di competenza. In tale quadro, il presidio tecnico-organizzativo fa capo in via principale alle strutture regionali competenti in materia di sistemi informativi, infrastrutture tecnologiche e cybersicurezza, con il coinvolgimento delle ulteriori strutture interessate per i profili di protezione dei dati personali, approvvigionamenti, esecuzione contrattuale, continuità operativa, comunicazione e gestione dei fornitori.

I processi e le attività di seguito riepilogati costituiscono il riferimento organizzativo unitario della **Regione Piemonte** ai fini dell'attuazione degli obblighi in materia di cybersicurezza.

I piani, le procedure e gli ulteriori documenti attuativi disciplinano le responsabilità e i raccordi necessari allo svolgimento dei rispettivi processi senza introdurre autonomamente ulteriori ruoli organizzativi permanenti rispetto a quelli definiti nel presente documento e negli atti organizzativi vigenti dell'Ente. Ove, per l'attuazione di uno specifico processo o per la gestione di un evento, sia necessario individuare una funzione operativa di coordinamento, questa è esercitata nell'ambito delle strutture e delle responsabilità organizzative competenti secondo quanto previsto dal relativo piano o procedura.

A. **Definizione delle policy in ambito cybersicurezza**

Le policy e gli altri documenti di governo della sicurezza informatica sono predisposti dal Settore A1911A - Sistema informativo regionale, con il coordinamento del Referente per la cybersicurezza e con il coinvolgimento delle strutture competenti per materia.

B. Continuità operativa e ripristino

La Regione Piemonte assicura la continuità operativa e il ripristino dei sistemi informativi e di rete rilevanti mediante processi distinti ma coordinati. Il Piano di continuità operativa disciplina le strategie e le misure organizzative finalizzate al mantenimento o al ripristino di livelli operativi accettabili dei servizi; il Piano di ripristino in caso di disastro disciplina il recupero delle componenti tecnologiche, dei sistemi e dei dati.

Per i profili specificamente attinenti alla cybersicurezza, il presidio tecnico-organizzativo è assicurato dal Settore A1911A - Sistema informativo regionale, in raccordo con il Settore A1910A - Servizi infrastrutturali e tecnologici, con le strutture regionali competenti per i servizi interessati e con i soggetti gestori, nei limiti dei rispettivi atti organizzativi, contratti, convenzioni o accordi di servizio.

Le misure di continuità e ripristino sono definite e aggiornate tenendo conto della criticità dei sistemi e dei servizi interessati, delle esigenze di continuità, delle dipendenze e degli esiti delle valutazioni del rischio. Le modalità operative sono disciplinate nei rispettivi piani e nelle procedure applicabili, senza duplicare le informazioni e la documentazione tecnica mantenute nelle fonti individuate dall'Ente.

C. Analisi e gestione dei rischi

Il processo di analisi e gestione dei rischi in ambito cybersicurezza è coordinato dal Settore **A1911A - Sistema informativo regionale**, con il coinvolgimento delle strutture regionali interessate e delle funzioni competenti per i profili di protezione dei dati personali, continuità operativa e gestione dei servizi.

Il processo comprende l'identificazione dei rischi, la valutazione del loro impatto e della loro probabilità, la definizione delle priorità di trattamento, l'individuazione delle misure di mitigazione e il riesame periodico del quadro dei rischi.

Le risultanze di tale processo costituiscono base di riferimento per la definizione delle misure organizzative, tecniche e procedurali necessarie a presidiare i sistemi informativi e di rete della **Regione Piemonte**.

D. Formazione in ambito cybersicurezza

Il Referente per la cybersicurezza promuove, con il supporto delle strutture regionali competenti per la formazione del personale, la definizione e l'attuazione di programmi di formazione e sensibilizzazione in materia di cybersicurezza rivolti al personale regionale [req. PR.AT-01]; detta formazione viene tracciata tramite gli strumenti in uso alla struttura per la formazione del personale [req. PR.AT-01.3].

Le iniziative formative e informative sono definite in modo proporzionato ai ruoli, alle responsabilità attribuite e ai livelli di esposizione al rischio, al fine di rafforzare la consapevolezza del personale e promuovere comportamenti coerenti con le politiche di sicurezza dell'Ente.

E. Gestione delle crisi

La gestione delle crisi costituisce un processo distinto rispetto alla gestione ordinaria degli incidenti, alla continuità operativa e al ripristino tecnologico ed è disciplinata dal Piano di gestione delle crisi.

Qualora un evento, per natura, estensione o impatti, richieda l'attivazione di meccanismi straordinari di coordinamento e decisione, si applicano i ruoli, le responsabilità e i raccordi previsti dal relativo Piano, nel rispetto dell'assetto organizzativo definito nel presente documento.
Il Piano di gestione delle crisi può essere attivato in coordinamento con il Piano di continuità operativa, con il Piano di ripristino in caso di disastro e con il processo di gestione degli incidenti, in relazione alle caratteristiche dell'evento; l'attivazione di uno di tali processi non determina automaticamente l'attivazione degli altri.

F. Gestione delle vulnerabilità

È definito, attuato, aggiornato e documentato un piano di gestione delle vulnerabilità che disciplina:

- le modalità per l'identificazione delle vulnerabilità e la pianificazione delle relative attività;
- le modalità per monitorare, ricevere, analizzare e rispondere alle informazioni sulle vulnerabilità;
- le procedure, i ruoli e le responsabilità per lo svolgimento delle attività di gestione delle vulnerabilità.

Il piano di gestione delle vulnerabilità è predisposto dal Settore **A1911A - Sistema informativo regionale**, con il coordinamento del Referente per la cybersicurezza, il coinvolgimento delle strutture tecniche interessate e, ove necessario, il supporto di fornitori o soggetti in house nei limiti dei relativi affidamenti.

G. Gestione degli incidenti

È definito, attuato, aggiornato e documentato un piano per la gestione degli incidenti di sicurezza informatica e delle relative notifiche, che disciplina:

- le fasi e le procedure di gestione e notifica degli incidenti, con l'indicazione dei relativi ruoli e delle responsabilità;
- le procedure per la predisposizione e la trasmissione delle relazioni e delle comunicazioni previste dalla normativa applicabile;
- le informazioni di contatto per la segnalazione degli incidenti;
- le modalità di comunicazione interna ed esterna;
- la reportistica da utilizzare per la documentazione dell'incidente.

Il piano per la gestione degli incidenti è predisposto dal Referente per la cybersicurezza, con il supporto del Settore **A1911A - Sistema informativo regionale**, del gruppo di lavoro interdirezionale e delle ulteriori strutture regionali competenti.
Nei casi di incidente con impatto su dati personali, sono coinvolti anche il **DPO**, la struttura competente in materia di privacy e i referenti privacy delle Direzioni interessate, secondo quanto previsto dagli atti interni dell'Ente.
Il piano è riesaminato e, se opportuno, aggiornato periodicamente e comunque almeno ogni due anni, nonché in occasione di incidenti significativi o di mutamenti dell'esposizione alle minacce e ai relativi rischi.

H. Gestione delle forniture con potenziali impatti sulla sicurezza

Il processo di affidamento di forniture, servizi e soluzioni con potenziali impatti sulla sicurezza dei sistemi informativi e di rete deve prevedere:

- il coinvolgimento delle strutture regionali competenti in materia di sistemi informativi, infrastrutture tecnologiche e cybersicurezza fin dalle fasi di identificazione e progettazione della fornitura;

- la definizione di requisiti di sicurezza coerenti con il livello di rischio associato alla fornitura e con le misure di sicurezza applicate dall'Ente;
- l'esplicitazione nei contratti, negli accordi di servizio e nella documentazione di gara degli obblighi di sicurezza posti a carico dei fornitori.

Per gli aspetti di programmazione, affidamento e presidio del contratto, rileva il ruolo del **RUP**, con il supporto delle strutture tecniche competenti; per i profili di esecuzione contrattuale rileva altresì il ruolo del **DEC**, ove nominato.
Eventuali ruoli e responsabilità in materia di sicurezza informatica assegnati al personale dei fornitori o di soggetti esterni sono esplicitati nei relativi contratti, accordi o documenti di servizio.

I. Notifiche all'autorità nazionale

Il Punto di contatto NIS2 e il relativo sostituto, formalmente individuati dall'Ente secondo gli atti di designazione vigenti, curano, nell'ambito delle rispettive attribuzioni, le interlocuzioni con l'autorità nazionale competente e assicurano la registrazione, la gestione e l'aggiornamento delle informazioni richieste dalla normativa applicabile.
Nell'ambito del processo di gestione degli incidenti, le interlocuzioni con lo CSIRT Italia e le notifiche previste dalla disciplina NIS sono effettuate dal Referente CSIRT e dagli eventuali sostituti, in raccordo con il Punto di contatto NIS, con il Referente per la cybersicurezza e con le strutture regionali interessate, secondo gli atti di designazione vigenti e le procedure interne dell'Ente.
Le notifiche e le interlocuzioni esterne sono effettuate secondo gli atti di nomina vigenti, le procedure interne dell'Ente e le modalità stabilite dalla normativa applicabile.

J. Monitoraggio e reporting

La **Regione Piemonte** assicura attività di monitoraggio e raccolta delle informazioni rilevanti ai fini della cybersicurezza, anche avvalendosi, nei limiti dei relativi affidamenti, di soggetti esterni o in house che svolgono servizi di supporto operativo o specialistico.
Le informazioni derivanti dal monitoraggio, dalle segnalazioni, dalle vulnerabilità e dagli incidenti sono analizzate dal Referente per la cybersicurezza e dalle strutture tecniche competenti al fine di identificare tendenze, aree critiche, necessità di intervento e possibili impatti sui servizi e sui sistemi dell'Ente.
Per i profili connessi ai dati personali, il **DPO** e la struttura competente in materia di privacy ricevono le informazioni rilevanti e valutano i necessari raccordi con le ulteriori strutture interessate. Gli esiti del monitoraggio e del reporting alimentano i flussi informativi interni e, ove necessario, supportano le notifiche e le comunicazioni verso l'esterno.

K. Revisione e miglioramento continuo

I ruoli e le strutture coinvolti nella gestione della sicurezza informatica della **Regione Piemonte**, nell'ambito delle rispettive competenze, contribuiscono all'individuazione di eventuali punti di debolezza del sistema organizzativo e di controllo e propongono interventi di miglioramento.
Gli interventi di miglioramento possono consistere, tra l'altro, nell'aggiornamento di policy e procedure, nell'adozione di nuove misure tecniche e organizzative, nella revisione delle responsabilità, nell'individuazione di nuovi rischi o nell'adeguamento delle misure di trattamento già previste.
Il riesame e il miglioramento continuo sono coordinati dal Referente per la cybersicurezza, con il supporto del Settore **A1911A - Sistema informativo regionale**, del gruppo di lavoro interdirezionale e delle ulteriori strutture competenti per materia; per i profili trasversali, i relativi

esiti sono portati all'attenzione del **Comitato di coordinamento direttori** ai fini del raccordo interdirezionale.

I processi e le attività sopra indicati sono attuati secondo il principio di proporzionalità, in relazione alla criticità dei servizi e dei sistemi interessati, alla natura dei dati e delle informazioni trattate, al ruolo delle strutture coinvolte e al livello di esposizione ai rischi della **Regione Piemonte**. Per i processi che comportano interazioni con soggetti esterni, affidamenti, servizi gestiti da terzi o supporto operativo di soggetti in house, restano comunque in capo alla **Regione Piemonte** le responsabilità organizzative, decisionali e di notifica previste dalla normativa applicabile.

5.3.2 RACI - Matrice attività / ruoli /responsabilità

Processo / attività	Comitato di coordinamento direttori	Settore A1911A - Sistema informativo regionale	Referente per la cybersicurezza	Punto di contatto NIS2	Referente CSIRT	DPO / struttura privacy	Strutture competenti per materia	RUP / DEC
Definizione policy in ambito cybersicurezza	C	R	A	I	I	C	C	
Gestione della continuità operativa	R	R	C	I	I	I	A	I
Analisi e gestione dei rischi	A	R	C	I	I	I	R	I
Formazione in ambito cybersicurezza	C	C	R	I			A	
Gestione delle crisi	A	R	C	I	I	C	R	I
Gestione delle vulnerabilità	I	R	A	I	R	I	R	R
Gestione degli incidenti	C	R	A	C	R	C	R	R
Gestione delle forniture con potenziali impatti sulla sicurezza	I	C	C				R	A
Notifiche all'autorità nazionale competente NIS	I	R	C	A	R		C	I
Monitoraggio e reporting	I	R	A	C	C	I	C	
Revisione e miglioramento continuo	A	R	R	I	I		C	

Si ricorda che tutti i dipendenti sono responsabili di osservare le politiche di sicurezza e di segnalare eventuali problemi o incidenti.

5.4 Tavoli di coordinamento

La **Regione Piemonte** assicura il coordinamento delle attività in materia di cybersicurezza mediante sedi di raccordo interdirezionale e tavoli operativi, attivati in coerenza con l'assetto organizzativo dell'Ente e con gli atti regionali vigenti.

In particolare, ai fini del raccordo interdirezionale sulle tematiche di cybersicurezza rilevano:

- il **Comitato di coordinamento direttori** di cui all'articolo 9, comma 4, della legge regionale 28 luglio 2008, n. 23 quale sede di raccordo tra le Direzioni regionali per l'esame delle tematiche trasversali e per l'acquisizione del parere sui documenti di governo della sicurezza informatica, secondo quanto previsto dal paragrafo 5.3;
- il **Gruppo di lavoro interdirezionale "Attuazione della normativa in materia di cybersicurezza"**, istituito con determinazione dirigenziale 22 gennaio 2025, n. 11/A1000A/2025, in attuazione della deliberazione della Giunta regionale 3 dicembre 2024, n. 3-474, quale tavolo operativo stabile di supporto al Referente per la cybersicurezza e di raccordo tra le strutture regionali coinvolte nell'attuazione degli obblighi in materia di cybersicurezza.

Il **Comitato di coordinamento direttori** costituisce la sede di riferimento per la trattazione dei profili che presentano rilievo trasversale per la **Regione Piemonte**, favorendo l'allineamento tra le Direzioni regionali, la condivisione delle priorità organizzative e il raccordo sulle misure da adottare. In tale ambito, il Comitato di coordinamento direttori è interessato, in particolare, per l'esame dei documenti di governo della sicurezza informatica, per i profili di coordinamento interdirezionale e per l'acquisizione del relativo parere, ferma restando l'adozione dei documenti da parte della struttura competente secondo la natura dell'atto.

Il **Gruppo di lavoro interdirezionale** opera quale sede tecnico-organizzativa di supporto all'attuazione degli adempimenti in materia di cybersicurezza e assicura, con il coordinamento del Referente per la cybersicurezza, il raccordo stabile tra le strutture regionali coinvolte. In tale ambito, il Gruppo di lavoro supporta:

- la presa in carico le segnalazioni di vulnerabilità e intervenga secondo i tempi e le disposizioni stabilite dalla norma;
- il rafforzamento delle misure di sicurezza dei dati;
- l'assolvimento agli obblighi di segnalazione e notifica degli incidenti informatici verso l'Agenzia per la cybersicurezza nazionale;

Ove necessario, in relazione a specifici processi, incidenti, vulnerabilità, forniture ICT o altri temi che richiedano approfondimenti specialistici, possono inoltre essere attivati momenti di coordinamento tematici o operativi tra le strutture regionali competenti, anche con il coinvolgimento dei soggetti esterni o in house che supportano l'Ente nei limiti dei relativi affidamenti. Tali momenti di raccordo non sostituiscono i tavoli formalizzati sopra richiamati e non modificano il riparto delle responsabilità organizzative previsto dal presente documento.

Le Direzioni regionali assicurano, nell'ambito delle rispettive competenze, la partecipazione ai tavoli di coordinamento sopra indicati e il tempestivo coinvolgimento delle strutture interessate, anche ai

fini della condivisione delle informazioni rilevanti, dell'attuazione delle misure concordate e del rispetto degli obblighi di segnalazione, gestione e notifica previsti dalla normativa applicabile.

5.5 Canali di comunicazione

La **Regione Piemonte** assicura che le comunicazioni rilevanti ai fini della cybersicurezza siano gestite in modo coordinato, tempestivo e coerente con l'assetto organizzativo dell'Ente, con la natura dell'evento e con gli obblighi previsti dalla normativa applicabile.

Le comunicazioni in materia di cybersicurezza si distinguono, in particolare, in:

- comunicazioni interne tra le strutture regionali coinvolte nei processi di prevenzione, gestione delle vulnerabilità, gestione degli incidenti, continuità operativa e gestione della crisi;
- comunicazioni verso l'autorità nazionale competente, verso lo **CSIRT Italia** e verso gli altri soggetti esterni competenti, nei casi e secondo le modalità previste dalla normativa applicabile;
- comunicazioni istituzionali esterne, nei casi in cui l'evento presenti rilievo pubblico, impatto reputazionale, effetti sui servizi o necessità di informazione verso utenti, cittadini, imprese o altri stakeholder.

Le comunicazioni interne sono assicurate secondo i flussi definiti nei documenti e nelle procedure dell'Ente e coinvolgono, in relazione alla natura dell'evento, il Referente per la cybersicurezza, il Settore **A1911A - Sistema informativo regionale**, il Punto di contatto NIS2, il referente CSIRT, le strutture tecniche interessate, il **DPO** e la struttura competente in materia di privacy, nonché le ulteriori Direzioni e strutture coinvolte per competenza.

Le comunicazioni verso l'autorità nazionale competente NIS sono curate dal Punto di contatto NIS2, con il supporto del relativo sostituto e delle strutture regionali interessate, secondo quanto previsto dagli atti di designazione vigenti, dalla normativa applicabile e dalle procedure interne dell'Ente. Le interlocuzioni con lo CSIRT Italia e le notifiche di incidente sono curate dal Referente CSIRT e dagli eventuali sostituti, in raccordo con il Punto di contatto NIS2, con il Referente per la cybersicurezza e con le strutture regionali interessate, secondo quanto previsto dagli atti di designazione vigenti e dalle procedure interne dell'Ente.

Nel caso di incidenti di particolare rilevanza pubblica o di potenziale impatto reputazionale, le modalità e i contenuti delle comunicazioni esterne istituzionali sono definiti dalle strutture regionali competenti in materia di comunicazione istituzionale, in raccordo con il **Gabinetto del Presidente della Giunta regionale**, con il Portavoce del Presidente e con il Referente per la cybersicurezza, tenendo conto della natura dell'evento, dei profili di riservatezza, degli impatti sui servizi e degli obblighi informativi applicabili.

Qualora l'autorità nazionale competente, ai sensi della normativa applicabile, intimi alla **Regione Piemonte** di informare il pubblico riguardo a un incidente informatico, l'Ente assicura una comunicazione tempestiva, coerente e proporzionata, coordinata tra le strutture tecniche e le strutture competenti in materia di comunicazione istituzionale, secondo quanto previsto dalle procedure interne e nel rispetto degli interessi pubblici coinvolti.

Nei casi di incidente che comportino anche violazione di dati personali, i flussi di comunicazione sono coordinati altresì con il **DPO**, con la struttura competente in materia di privacy e con i referenti privacy delle Direzioni interessate, secondo quanto previsto dagli atti interni dell'Ente in materia di protezione dei dati personali.

6. AGGIORNAMENTO

Il presente documento è riesaminato e, ove necessario, aggiornato periodicamente e comunque almeno ogni due anni, nonché ogniqualvolta si verifichino, per gli ambiti di competenza, evoluzioni del contesto normativo in materia di cybersicurezza, incidenti significativi, variazioni organizzative, modifiche del perimetro dei servizi e dei sistemi interessati o mutamenti dell'esposizione ai rischi.

Le proposte di aggiornamento del documento sono predisposte dal Settore A1911A - Sistema informativo regionale, con il coordinamento del Referente per la cybersicurezza e con il supporto del gruppo di lavoro interdirezionale, per quanto di competenza.

Le modifiche e le integrazioni di carattere sostanziale sono sottoposte al Comitato di coordinamento direttori ai fini del raccordo interdirezionale. Le modifiche di carattere meramente formale, redazionale o di aggiornamento non sostanziale, ivi incluse quelle finalizzate all'aggiornamento di denominazioni organizzative, riferimenti interni o rinvii documentali che non incidano sul contenuto sostanziale del documento, possono essere disposte dalla struttura competente secondo l'assetto organizzativo vigente, con successiva informativa al primo Comitato di coordinamento direttori utile.

Gli aggiornamenti del documento sono tracciati secondo le modalità organizzative adottate dall'Ente per la gestione della documentazione interna.

7. PUBBLICAZIONE

Il presente documento è reso disponibile nell'ambito dei sistemi documentali interni della Regione Piemonte e nei canali interni dell'Ente individuati per la consultazione della documentazione organizzativa e procedurale in materia di cybersicurezza.

La diffusione del documento è assicurata nei confronti delle strutture regionali e dei soggetti interni interessati, in relazione alle rispettive competenze e responsabilità.

La pubblicazione esterna di ulteriori contenuti del presente documento è valutata dall'Ente secondo criteri di pertinenza, proporzionalità e tutela delle informazioni organizzative e di sicurezza.

VERIFICHE ED APPROVAZIONI

VER.	REDAZIONE		CONTROLLO ED APPROVAZIONE		AUTORIZZAZIONE ALL'EMISSIONE	
	NOME	DATA	NOME	DATA	NOME	DATA
V01						

STATO DELLE VARIAZIONI

VER.	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
V01	Tutto il documento	Versione iniziale del documento

INDICE

ACRONIMI **2**

1 INTRODUZIONE **3**

1.1 GENERALITÀ E OBIETTIVO 3
1.2 CAMPO DI APPLICAZIONE 3

2 POLITICHE DI SICUREZZA INFORMATICA PER AMBITO **4**

2.1 PRINCIPI GENERALI SULLA SICUREZZA DELLE INFORMAZIONI 4
2.2 GOVERNO DELLA SICUREZZA E GESTIONE DEL RISCHIO 4
2.3 RUOLI, RESPONSABILITÀ E AFFIDABILITÀ DELLE PERSONE 5
2.4 FORMAZIONE E CONSAPEVOLEZZA 5
2.5 GESTIONE DEGLI ASSET 5
2.6 IDENTITÀ DIGITALI E CONTROLLO DEGLI ACCESSI 6
2.7 SICUREZZA DEI DATI E CONTROLLI CRITTOGRAFICI 6
2.8 SICUREZZA FISICA E AMBIENTALE 7
2.9 SICUREZZA DELLE ATTIVITÀ OPERATIVE 7
2.10 GESTIONE DELLE VULNERABILITÀ 7
2.11 MONITORAGGIO DEGLI EVENTI DI SICUREZZA 8
2.12 SICUREZZA DELLE RETI E DEI SISTEMI 8
2.13 SICUREZZA DELLA CATENA DI APPROVVIGIONAMENTO ICT E RAPPORTI CON LE TERZE PARTI 8
2.14 GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA 9
2.15 CONTINUITÀ OPERATIVA, DISASTER RECOVERY E GESTIONE DELLE CRISI 9
2.16 CONFORMITÀ E AUDIT DI SICUREZZA 10
2.17 ACQUISIZIONE, SVILUPPO, CONFIGURAZIONE, MANUTENZIONE E DISMISSIONE 10

RIFERIMENTI NORMATIVI E DOCUMENTALI **10**

DEFINIZIONI

TERMINE	DEFINIZIONE
Asset	Risorsa, fisica o logica, rilevante per la sicurezza informatica dell'ente, inclusi sistemi, apparati, applicazioni, servizi digitali, banche dati, informazioni, componenti infrastrutturali, dispositivi e ulteriori risorse ict.
Autenticazione	Processo attraverso il quale viene verificata l'identità di un utente, dispositivo, servizio o processo che richiede accesso a un sistema, a un'applicazione o a una risorsa informativa.
Autorizzazione	Processo attraverso il quale sono attribuiti, modificati, verificati o revocati i diritti di accesso a sistemi, dati, applicazioni, reti e servizi digitali.
Disponibilità	Proprietà per cui sistemi, dati e servizi sono accessibili e utilizzabili dai soggetti autorizzati nei tempi e secondo le modalità previste.
Incidente di sicurezza informatica	Evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso essi.
Informazioni	Dati, documenti, comunicazioni, registrazioni, configurazioni, evidenze tecniche e ulteriori contenuti trattati dall'ente nell'ambito dei propri processi istituzionali, amministrativi e digitali.
Integrità	Proprietà per cui le informazioni e i sistemi sono accurati, completi e protetti da modifiche non autorizzate o non corrette.
Politica di sicurezza informatica	Insieme di principi, indirizzi e regole generali adottati dall'ente per orientare la protezione dei sistemi informativi e di rete, delle informazioni trattate e dei servizi digitali erogati.
Riservatezza	Proprietà per cui le informazioni sono accessibili esclusivamente ai soggetti autorizzati e per le finalità consentite.
Rischio informatico	Combinazione della probabilità che una minaccia sfrutti una vulnerabilità e dell'impatto che tale evento può produrre sui sistemi, sui dati, sui servizi o sull'operatività dell'ente.
Sistema informativo e di rete	Insieme di reti, dispositivi, sistemi, applicazioni, servizi e dati digitali utilizzati per il funzionamento, l'erogazione, la protezione e la manutenzione dei servizi dell'ente.
Terza parte	Soggetto diverso dall'ente che, in forza di contratto, convenzione, incarico, accordo di servizio o altro atto regolativo, accede a sistemi, dati, infrastrutture o servizi ict dell'ente, oppure concorre alla loro gestione, manutenzione, sviluppo, erogazione o protezione.
Tracciabilità	Capacità di registrare e ricostruire operazioni, accessi, modifiche, eventi e decisioni rilevanti ai fini della sicurezza informatica.
Vulnerabilità	Debolezza, difetto o configurazione non adeguata di un sistema, servizio, processo o componente ict che può essere sfruttata da una minaccia informatica.

ACRONIMI

Acronimo	Descrizione
ACN	Agenzia per la Cybersicurezza Nazionale
CSIRT	Computer Security Incident Response Team
DPO	Data Protection Officer / Responsabile della protezione dei dati
DR	Disaster Recovery
ICT	Information and Communication Technology
MFA	Multi-Factor Authentication / Autenticazione multifattore
NIS	Network and Information Security

PdC	Punto di contatto NIS
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SOC	Security Operations Center
VPN	Virtual Private Network

1 Introduzione

1.1 Generalità e obiettivo

Il presente documento, predisposto anche ai fini dell'attuazione della misura GV.PO-01 delle Specifiche di base NIS, definisce i principi generali e le politiche di sicurezza informatica adottate da Regione Piemonte per la protezione dei sistemi informativi e di rete, delle informazioni trattate e dei servizi digitali erogati.

La Politica costituisce il livello generale di indirizzo dell'impianto documentale di sicurezza informatica dell'Ente. I piani disciplinano, nei rispettivi ambiti, gli obiettivi, i criteri, le strategie e le modalità di governo dei processi; le procedure definiscono le modalità operative comuni di attuazione; le eventuali istruzioni tecniche e i runbook dettagliano, ove necessario, le attività esecutive riferite a specifici sistemi, tecnologie o servizi.

Le informazioni soggette a frequente variazione e le evidenze operative sono mantenute nei registri, negli inventari, nei sistemi gestionali o nelle ulteriori fonti individuate dall'Ente, evitando per quanto possibile la duplicazione delle medesime informazioni nei diversi documenti.

Le disposizioni contenute nel presente documento sono definite secondo un approccio proporzionato al contesto organizzativo, tecnico e operativo dell'Ente, tenendo conto della criticità dei servizi erogati, dei rischi per la sicurezza informatica, degli obblighi normativi applicabili e delle risorse disponibili.

La Politica è finalizzata a garantire un quadro coerente di indirizzo per la protezione della riservatezza, integrità, disponibilità e autenticità delle informazioni, nonché per la prevenzione, il rilevamento, la gestione e il ripristino a fronte di eventi e incidenti di sicurezza informatica.

Il documento è riesaminato e, ove opportuno, aggiornato periodicamente e comunque almeno con cadenza annuale, nonché qualora si verifichino evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi. Nell'ambito del riesame è verificata almeno la conformità delle politiche alla normativa applicabile e i relativi esiti sono tracciati secondo le modalità adottate dall'Ente.

1.2 Campo di applicazione

La presente Politica si applica ai sistemi informativi e di rete, alle infrastrutture tecnologiche, agli applicativi, alle banche dati, ai servizi digitali e alle informazioni trattate da Regione Piemonte, indipendentemente dalla modalità di gestione, interna o affidata a soggetti terzi.

Le disposizioni si applicano al personale dell'Ente e, nei limiti previsti da contratti, convenzioni, incarichi, accordi di servizio o altri atti regolativi, ai collaboratori, ai fornitori, ai soggetti terzi e agli altri soggetti che accedono ai sistemi informativi dell'Ente, trattano informazioni per conto dell'Ente o concorrono alla gestione, manutenzione, sviluppo, erogazione o protezione dei servizi ICT.

Rientrano nel campo di applicazione della presente Politica le attività connesse alla gestione delle informazioni, dei processi e delle risorse utilizzate per la progettazione, l'acquisizione, la realizzazione, l'avviamento, l'erogazione, la manutenzione e la dismissione dei servizi digitali dell'Ente.

La Politica si applica inoltre alle attività di cooperazione, interoperabilità, scambio informativo e integrazione con altri enti, amministrazioni, società in house, fornitori, partner tecnologici o soggetti terzi, quando tali attività comportino accesso a sistemi, dati, servizi o infrastrutture dell'Ente.

Per i servizi, i sistemi o le componenti gestiti da soggetti esterni, l'applicazione dei principi contenuti nel presente documento è assicurata attraverso gli strumenti contrattuali, convenzionali e organizzativi applicabili, in coerenza con il ruolo svolto dal soggetto esterno e con il livello di rischio associato al servizio o alla fornitura.

Le modalità operative di attuazione della presente Politica sono disciplinate dai piani, dalle procedure, dalle istruzioni operative e dagli ulteriori documenti collegati adottati dall'Ente.

2 Politiche di sicurezza informatica per ambito

2.1 Principi generali sulla sicurezza delle informazioni

Regione Piemonte adotta politiche, misure organizzative e presidi tecnici finalizzati a proteggere i sistemi informativi e di rete, le informazioni trattate e i servizi digitali erogati, secondo criteri di proporzionalità rispetto al contesto organizzativo, alla criticità dei servizi e ai rischi rilevati.

La sicurezza delle informazioni è orientata alla tutela dei seguenti principi:

- riservatezza, affinché le informazioni siano accessibili esclusivamente ai soggetti autorizzati e per le finalità consentite;
- integrità, affinché le informazioni siano accurate, complete e protette da modifiche non autorizzate o non corrette;
- disponibilità, affinché sistemi, dati e servizi siano accessibili e utilizzabili nei tempi e secondo le modalità previste;
- autenticità, affinché sia possibile verificare l'identità dei soggetti e l'origine delle informazioni;
- tracciabilità, affinché le operazioni rilevanti siano registrate e ricostruibili, nel rispetto delle regole applicabili.

Le misure di sicurezza sono definite e attuate tenendo conto degli obblighi normativi applicabili, delle indicazioni delle Autorità competenti, degli esiti dell'analisi del rischio, delle caratteristiche dei servizi erogati, dell'organizzazione dell'Ente e delle risorse disponibili.

La protezione delle informazioni comprende anche, ove applicabile, la tutela dei dati personali trattati dall'Ente, nel rispetto della disciplina in materia di protezione dei dati personali e in coordinamento con le funzioni competenti.

2.2 Governo della sicurezza e gestione del rischio

Le politiche di sicurezza informatica dell'Ente sono definite e attuate secondo un approccio basato sul rischio, tenendo conto della criticità dei servizi istituzionali e digitali, dei sistemi informativi e di rete, delle informazioni trattate, delle dipendenze da terze parti e degli scenari di minaccia rilevanti.

Gli esiti della valutazione del rischio indirizzano la definizione delle priorità di trattamento, l'individuazione delle misure di sicurezza e la pianificazione degli interventi necessari, alimentando in modo coordinato il processo di trattamento dei rischi e il piano di adeguamento dell'Ente.
La valutazione del rischio informatico è disciplinata dal **[REGP_PIA03] Valutazione del rischio cyber**, che definisce le modalità di identificazione, analisi, ponderazione e riesame dei rischi. Le decisioni relative al trattamento dei rischi individuati sono disciplinate dal **[REGP_PIA04] Piano di trattamento dei rischi** per la

sicurezza informatica. Gli interventi di adeguamento conseguenti alle valutazioni effettuate e alle ulteriori esigenze di conformità e miglioramento sono pianificati e monitorati attraverso il **[REGP_PIA05] Piano di adeguamento NIS2**.

2.3 RUOLI, RESPONSABILITÀ E AFFIDABILITÀ DELLE PERSONE

I ruoli, le responsabilità, i correlati poteri e i raccordi funzionali rilevanti per la sicurezza informatica, nonché i criteri relativi all'assegnazione dei ruoli, alle competenze e all'affidabilità delle persone coinvolte, sono definiti nel **[REGP_POL01] Organizzazione per la sicurezza informatica** e negli ulteriori atti organizzativi applicabili.

Il personale dell'Ente, i collaboratori, i fornitori e gli altri soggetti che accedono a sistemi, dati o servizi ICT dell'Ente operano nel rispetto delle responsabilità loro attribuite, delle presenti politiche, delle procedure, degli obblighi contrattuali o convenzionali e delle istruzioni operative applicabili.

2.4 FORMAZIONE E CONSAPEVOLEZZA

Regione Piemonte promuove la formazione e la consapevolezza del personale sui temi della sicurezza informatica, al fine di favorire comportamenti corretti, ridurre il rischio derivante da errori umani e rafforzare la capacità dell'organizzazione di prevenire, riconoscere e segnalare eventi rilevanti per la sicurezza.

Le attività di formazione e sensibilizzazione sono pianificate tenendo conto dei ruoli, delle responsabilità e del livello di esposizione al rischio delle diverse categorie di personale. Specifiche attività formative sono previste per il personale con compiti tecnici, amministrativi, gestionali o decisionali rilevanti per la sicurezza informatica.

Il personale dell'Ente è tenuto a conoscere e rispettare le politiche, le procedure e le istruzioni operative applicabili nell'utilizzo dei sistemi informativi, degli strumenti digitali, delle informazioni e dei servizi ICT messi a disposizione dall'Amministrazione.

Le modalità di pianificazione, erogazione, tracciamento, riesame e aggiornamento delle attività formative sono definite nel ***[REGP_PIA06] Piano Formazione Cybersecurity***.

2.5 GESTIONE DEGLI ASSET

Regione Piemonte mantiene inventari aggiornati degli asset rilevanti per la sicurezza informatica, comprendenti, secondo il perimetro definito dall'Ente, sistemi, apparati fisici, postazioni di lavoro, dispositivi mobili, piattaforme, applicazioni software, banche dati, servizi digitali, componenti infrastrutturali e ulteriori risorse ICT.

Gli asset sono censiti, classificati e gestiti secondo criteri coerenti con la loro criticità, con le informazioni trattate, con i servizi supportati e con il livello di rischio associato. Per ciascun asset o categoria di asset sono individuate le strutture competenti per la gestione, l'aggiornamento, la protezione e l'eventuale dismissione.

A supporto delle attività di censimento, Regione Piemonte utilizza, tra gli strumenti disponibili, una piattaforma di asset management basata su CMDBuild, operativa in produzione e dedicata all'inventario delle soluzioni software realizzate da CSI Piemonte o acquisite da altri fornitori per conto dell'Ente.

L'accesso alla rete, l'installazione di software, l'utilizzo di dispositivi e l'attivazione di servizi ICT avvengono secondo modalità autorizzate e tracciabili, nel rispetto delle procedure adottate dall'Ente.

Gli utenti sono tenuti a utilizzare gli asset assegnati esclusivamente per finalità istituzionali o comunque autorizzate, adottando comportamenti coerenti con le regole interne e con le misure di sicurezza previste.

La dismissione, la sostituzione, il riuso o lo smaltimento degli asset avvengono assicurando la protezione delle informazioni eventualmente contenute, anche attraverso misure di cancellazione sicura, restituzione, revoca degli accessi e aggiornamento degli inventari.

2.6 IDENTITÀ DIGITALI E CONTROLLO DEGLI ACCESSI

L'accesso ai sistemi informativi, alle applicazioni, alle reti, ai dati e ai servizi digitali dell'Ente è consentito esclusivamente ai soggetti autorizzati, secondo modalità coerenti con il ruolo svolto, le esigenze operative e il principio del privilegio minimo.

La gestione del ciclo di vita delle identità digitali e delle abilitazioni prevede modalità formalizzate per la richiesta, l'autorizzazione, l'attivazione, la modifica, la verifica periodica e la revoca degli accessi.

Le identità digitali sono di norma individuali e riconducibili al soggetto utilizzatore. Eventuali eccezioni, motivate da esigenze tecniche o organizzative, sono autorizzate, documentate e presidiate mediante misure idonee a garantire responsabilità, tracciabilità e controllo.

I diritti di accesso sono attribuiti sulla base delle effettive necessità operative, nel rispetto dei principi di separazione delle funzioni, privilegio minimo e necessità di conoscere. Le utenze con privilegi elevati sono censite, autorizzate, utilizzate solo quando necessario e sottoposte a controlli proporzionati alla criticità delle attività svolte.

Gli accessi da remoto sono autorizzati, protetti mediante misure adeguate e monitorati in relazione alla criticità dei sistemi e dei servizi interessati. Per gli accessi ai sistemi informativi e di rete rilevanti e per gli accessi effettuati mediante utenze con privilegi elevati sono adottate misure di autenticazione rafforzata coerenti con i requisiti applicabili, con gli esiti della valutazione del rischio e con le caratteristiche dei sistemi interessati.

In caso di cessazione del rapporto di lavoro, variazione di ruolo, modifica dell'incarico o venir meno delle esigenze operative, le abilitazioni sono aggiornate o revocate tempestivamente secondo le procedure adottate dall'Ente.

2.7 SICUREZZA DEI DATI E CONTROLLI CRITTOGRAFICI

Regione Piemonte protegge i dati e le informazioni trattati nei propri sistemi informativi e di rete mediante misure organizzative e tecniche proporzionate alla natura delle informazioni, alla criticità dei servizi supportati e ai rischi rilevati.

La protezione riguarda l'intero ciclo di vita delle informazioni, incluse le fasi di creazione, raccolta, accesso, elaborazione, conservazione, trasmissione, condivisione, archiviazione e cancellazione.

Le misure di protezione possono includere controlli di accesso, segregazione, tracciabilità, backup, protezione dei supporti, cifratura e ulteriori presidi coerenti con la classificazione delle informazioni e con il livello di rischio.

L'Ente valuta e adotta misure crittografiche proporzionate al rischio, alla criticità dei sistemi, alla classificazione delle informazioni e alla natura dei dati trattati, con particolare riferimento a dati conservati, dati trasmessi, dispositivi mobili, supporti rimovibili, backup, credenziali, comunicazioni da remoto e ulteriori componenti o flussi informativi che richiedano specifiche garanzie di riservatezza, integrità o autenticità.

L'utilizzo di strumenti crittografici avviene secondo modalità coerenti con le indicazioni tecniche e organizzative definite dall'Ente, assicurando la corretta gestione delle chiavi, delle credenziali, dei certificati e degli strumenti utilizzati.

2.8 SICUREZZA FISICA E AMBIENTALE

Regione Piemonte protegge gli ambienti, i locali, le apparecchiature e le infrastrutture che ospitano o supportano sistemi informativi e servizi ICT mediante misure fisiche e ambientali proporzionate alla criticità degli asset e dei servizi interessati.

L'accesso ai locali tecnici, alle aree riservate e agli spazi in cui sono presenti apparati o informazioni rilevanti è controllato e limitato ai soggetti autorizzati. Le misure adottate possono includere controlli di accesso fisico, registrazione degli accessi, protezione da furto o manomissione, misure antincendio, continuità elettrica, climatizzazione e ulteriori presidi ambientali.

Per i sistemi, i servizi o le infrastrutture gestiti da terze parti, incluse società in house, fornitori cloud, data center esterni o altri soggetti affidatari, i requisiti di sicurezza fisica e ambientale sono disciplinati dagli accordi, dai contratti, dalle convenzioni o dagli altri atti applicabili.

Gli asset mobili e portatili sono custoditi e utilizzati in modo da ridurre il rischio di furto, smarrimento, accesso non autorizzato o compromissione delle informazioni trattate.

2.9 SICUREZZA DELLE ATTIVITÀ OPERATIVE

Regione Piemonte assicura che l'esercizio dei sistemi informativi e dei servizi ICT avvenga secondo modalità controllate, documentate e coerenti con le esigenze di sicurezza, continuità e affidabilità dei servizi.

Le attività operative prevedono misure adeguate alla gestione delle configurazioni, il controllo delle modifiche, la protezione da codice malevolo, la gestione dei backup, la manutenzione dei sistemi e la tracciabilità delle attività rilevanti.

Le modifiche ai sistemi, alle applicazioni, alle configurazioni e alle infrastrutture ICT sono gestite mediante processi formalizzati, che consentono la valutazione degli impatti, l'autorizzazione, l'esecuzione controllata, la verifica degli esiti e la tracciabilità delle attività svolte.

I sistemi e gli strumenti di protezione dal codice malevolo sono mantenuti aggiornati e configurati in modo coerente con il livello di rischio e con le caratteristiche degli asset da proteggere.

Le attività di backup sono pianificate, eseguite e verificate in relazione alla criticità dei dati, dei sistemi e dei servizi supportati. Sono definite modalità di conservazione e ripristino coerenti con gli obiettivi di continuità operativa e con le esigenze di protezione delle informazioni.

Le attività operative svolte da fornitori, società in house o altri soggetti terzi sono disciplinate dagli accordi, dai contratti o dagli atti applicabili, in coerenza con le politiche di sicurezza dell'Ente e con il livello di rischio associato ai servizi affidati.

2.10 GESTIONE DELLE VULNERABILITÀ

Regione Piemonte adotta politiche e processi per l'identificazione, la valutazione, la prioritizzazione e il trattamento delle vulnerabilità che interessano sistemi informativi e di rete, applicazioni, infrastrutture, servizi digitali e componenti tecnologiche.

Le vulnerabilità sono gestite secondo criteri proporzionati alla criticità degli asset e dei servizi interessati, agli esiti dell'analisi del rischio, alle informazioni provenienti da fonti interne ed esterne e alle eventuali segnalazioni delle Autorità competenti.

Il trattamento delle vulnerabilità può prevedere, in funzione del contesto e del rischio associato, l'applicazione di aggiornamenti di sicurezza, l'adozione di misure di mitigazione, la limitazione dell'esposizione, la sostituzione di componenti non adeguate o l'accettazione documentata del rischio residuo secondo le modalità definite dall'Ente.

Le modalità operative di identificazione, analisi, trattamento, monitoraggio e rendicontazione delle vulnerabilità sono disciplinate nel ***[REGP_PIA02] Piano di gestione delle vulnerabilità*** e nei relativi documenti attuativi.

2.11 MONITORAGGIO DEGLI EVENTI DI SICUREZZA

Regione Piemonte assicura, in misura proporzionata al rischio e alla criticità dei sistemi e dei servizi, il monitoraggio degli eventi rilevanti per la sicurezza informatica, al fine di rilevare tempestivamente anomalie, comportamenti sospetti, accessi non autorizzati, codice malevolo, indisponibilità o altri eventi potenzialmente idonei a compromettere la sicurezza dei sistemi informativi e di rete.

Le attività di monitoraggio si basano sulla raccolta, conservazione e analisi dei log e delle altre evidenze tecniche disponibili, nel rispetto delle regole applicabili e delle responsabilità definite dall'Ente.

I sistemi, i servizi e gli eventi oggetto di monitoraggio sono individuati tenendo conto della criticità degli asset, degli esiti dell'analisi del rischio, dei livelli di servizio attesi, delle capacità tecniche disponibili e degli obblighi applicabili.

Le evidenze derivanti dal monitoraggio sono utilizzate per supportare le attività di rilevamento, analisi, gestione degli incidenti, gestione delle vulnerabilità, verifica dell'efficacia delle misure e miglioramento continuo.

2.12 SICUREZZA DELLE RETI E DEI SISTEMI

Regione Piemonte protegge le reti, i sistemi e le infrastrutture ICT mediante misure tecniche e organizzative finalizzate a prevenire accessi non autorizzati, limitare la propagazione di eventuali compromissioni e garantire la disponibilità dei servizi.
Le reti sono progettate, configurate e mantenute secondo criteri di sicurezza proporzionati alla criticità dei servizi e delle informazioni trattate. Ove necessario, sono previste misure di segmentazione, filtraggio, controllo del traffico, protezione perimetrale e separazione degli ambienti.
Le interconnessioni tra reti interne, reti pubbliche, ambienti cloud, sedi dell'Ente, reti di fornitori, società in house o altri soggetti terzi sono autorizzate, documentate e protette mediante presidi adeguati.
I sistemi server, le postazioni di lavoro, i dispositivi mobili, gli apparati di rete e gli ulteriori endpoint sono configurati e mantenuti secondo criteri di sicurezza, aggiornamento, controllo degli accessi, protezione da minacce informatiche e riduzione della superficie di attacco.
Le connessioni da remoto avvengono tramite canali autorizzati e protetti, con misure di autenticazione e controllo commisurate alla criticità dei sistemi e delle attività svolte.

2.13 SICUREZZA DELLA CATENA DI APPROVVIGIONAMENTO ICT E RAPPORTI CON LE TERZE PARTI

I rapporti con fornitori, società in house, partner tecnologici e altri soggetti terzi che accedono a sistemi, dati, infrastrutture o servizi ICT dell'Ente sono regolati da contratti, convenzioni, accordi di servizio o altri atti idonei, contenenti requisiti di sicurezza informatica proporzionati alla natura del servizio e al rischio associato.
Tali atti prevedono, ove applicabile, obblighi in materia di riservatezza, protezione delle informazioni, sicurezza dei sistemi, gestione degli accessi, continuità del servizio, gestione degli incidenti, cooperazione con l'Ente, tracciabilità delle attività, subfornitura, localizzazione o trattamento dei dati e facoltà di verifica o audit.
I fornitori e le terze parti sono gestiti tenendo conto della criticità dei servizi affidati, del livello di accesso riconosciuto, delle informazioni trattate, della dipendenza operativa dell'Ente dal servizio o dalla fornitura e degli esiti della valutazione del rischio.

I requisiti di sicurezza sono considerati, ove pertinenti, nelle fasi di pianificazione, acquisizione, affidamento, esecuzione, modifica e cessazione dei servizi ICT.
Specifici accordi di riservatezza possono essere previsti quando necessari in relazione alla natura delle informazioni trattate, al livello di accesso riconosciuto alla terza parte o alle caratteristiche del servizio affidato.

2.14 GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA

Regione Piemonte adotta un processo strutturato per la gestione degli eventi e degli incidenti di sicurezza informatica, finalizzato a rilevare, analizzare, classificare, contenere, risolvere, documentare e riesaminare gli eventi che possono compromettere la sicurezza dei sistemi informativi e di rete, delle informazioni trattate o dei servizi erogati.

Il processo di gestione degli incidenti prevede ruoli e responsabilità, canali di segnalazione, criteri di classificazione, modalità di escalation, attività di risposta, comunicazioni interne ed esterne, eventuali notifiche verso le Autorità competenti, attività di ripristino e raccolta delle lezioni apprese.

Le modalità operative di gestione degli incidenti, incluse le attività di rilevamento, risposta, contenimento, eradicazione, ripristino, notifica e rendicontazione, sono disciplinate nel ***[REGP_PIA01] Piano di gestione degli incidenti di sicurezza informatica*** e nei relativi documenti attuativi.

2.15 CONTINUITÀ OPERATIVA, DISASTER RECOVERY E GESTIONE DELLE CRISI

Regione Piemonte assicura la resilienza dei sistemi informativi e di rete rilevanti mediante processi distinti ma coordinati di continuità operativa, ripristino in caso di disastro e gestione delle crisi, applicati secondo criteri proporzionati alla criticità dei servizi, agli impatti attesi, alle dipendenze e agli esiti della valutazione del rischio.

Il Piano di continuità operativa disciplina le strategie e le misure organizzative finalizzate al mantenimento o al ripristino di livelli operativi accettabili dei servizi. Il Piano di ripristino in caso di disastro disciplina le strategie e le modalità di recupero delle componenti tecnologiche, dei sistemi e dei dati. Il Piano di gestione delle crisi disciplina i meccanismi straordinari di coordinamento, decisione ed escalation richiesti dagli eventi di particolare gravità.

I tre processi possono essere attivati singolarmente o in modo coordinato in relazione alla natura, all'estensione e agli impatti dell'evento; l'attivazione di uno di essi non determina automaticamente l'attivazione degli altri. Il raccordo con il processo di gestione degli incidenti è assicurato quando l'evento abbia natura cyber o presenti caratteristiche rilevanti ai fini della sicurezza informatica.

Per i sistemi e i servizi rilevanti sono individuati, ove applicabili, criticità, priorità, dipendenze e obiettivi di continuità e ripristino, inclusi RTO, RPO e ulteriori parametri definiti dall'Ente. Le informazioni comuni e soggette a variazione sono mantenute in fonti condivise individuate dall'Ente, in modo da evitarne la duplicazione nei diversi piani.

Le procedure operative comuni sono disciplinate nel REGP_PR01 – Procedure per la sicurezza informatica. Le istruzioni, le configurazioni e i runbook tecnici riferiti a specifici sistemi o servizi possono essere mantenuti dalle strutture competenti, da CSI Piemonte o dagli ulteriori soggetti gestori, purché siano identificabili, aggiornati, accessibili ai soggetti autorizzati e coerenti con gli obiettivi e i requisiti definiti dall'Ente.

L'efficacia delle misure di continuità, ripristino e gestione delle crisi è verificata mediante attività di test ed esercitazione proporzionate alla criticità dei servizi e ai rischi rilevati; gli esiti delle verifiche concorrono al riesame e al miglioramento dei relativi piani, procedure e misure.

2.16 Conformità e audit di sicurezza

Regione Piemonte assicura che le politiche, i processi e le misure di sicurezza informatica siano definiti, attuati e aggiornati tenendo conto del quadro normativo e regolatorio applicabile, delle indicazioni delle Autorità competenti e degli obblighi rilevanti per l'Amministrazione.

La conformità riguarda, in particolare, la disciplina in materia di cybersicurezza, amministrazione digitale, protezione dei dati personali, contratti pubblici, gestione documentale, continuità dei servizi digitali e ulteriori disposizioni applicabili in relazione alla natura dell'Ente e dei servizi erogati.

L'Ente promuove attività di verifica, riesame e miglioramento delle misure di sicurezza informatica, anche sulla base degli esiti di audit, controlli interni, analisi del rischio, incidenti, cambiamenti organizzativi o tecnologici e aggiornamenti normativi.

Gli esiti delle attività di verifica e riesame sono documentati secondo le modalità adottate dall'Ente e possono determinare l'aggiornamento delle politiche, dei piani, delle procedure, delle misure tecniche e organizzative o delle priorità di intervento.

Eventuali deroghe, eccezioni o scostamenti rispetto alle politiche di sicurezza sono motivati, documentati, autorizzati secondo le responsabilità definite dall'Ente e sottoposti a riesame periodico.

2.17 Acquisizione, sviluppo, configurazione, manutenzione e dismissione

L'acquisizione, lo sviluppo, la configurazione, la manutenzione, l'evoluzione e la dismissione di sistemi, applicazioni, infrastrutture e servizi ICT sono gestiti secondo criteri di sicurezza, qualità, tracciabilità e controllo del rischio.

La sicurezza informatica è considerata sin dalle fasi di pianificazione, progettazione, acquisizione o sviluppo di nuovi sistemi e servizi, anche mediante l'applicazione dei principi di sicurezza e protezione dei dati fin dalla progettazione e per impostazione predefinita, ove applicabili.

Le modifiche ai sistemi informativi, agli applicativi, alle configurazioni e alle infrastrutture sono autorizzate, documentate, testate e rilasciate secondo modalità controllate, tenendo conto degli impatti sulla sicurezza, sulla continuità operativa e sull'integrità dei dati.

Le componenti software, le configurazioni, le dipendenze tecnologiche e le applicazioni in uso sono gestite in modo da consentire il controllo delle versioni, l'individuazione di componenti non autorizzate, la gestione delle vulnerabilità e la pianificazione degli aggiornamenti.

I sistemi non più supportati o non più adeguati rispetto ai requisiti di sicurezza sono sostituiti, aggiornati, isolati o protetti mediante misure compensative, secondo priorità definite in base al rischio e alla criticità dei servizi interessati.

Le modalità operative relative all'acquisizione, allo sviluppo, alla configurazione, alla manutenzione, alla gestione delle modifiche e alla dismissione sono disciplinate, secondo il rispettivo ambito di competenza, dai processi regionali, dagli strumenti contrattuali o convenzionali e dalle procedure tecniche adottate dai fornitori e dai gestori dei servizi. Regione Piemonte assicura che le esigenze di sicurezza informatica siano considerate nei processi di propria competenza e nei requisiti applicabili ai servizi affidati.

Riferimenti normativi e documentali

Le politiche di sicurezza informatica definite nel presente documento sono adottate in coerenza con il quadro normativo e regolatorio applicabile all'Ente, come richiamato nel **REGP_POL01 – Organizzazione per la sicurezza informatica** e negli ulteriori documenti dell'impianto documentale di sicurezza.
Il presente documento si raccorda, in particolare, con i seguenti documenti:

Codice	Documento	Ambito
REGP_POL01	**Organizzazione per la sicurezza informatica**	Governance, ruoli, responsabilità e raccordi organizzativi
REGP_PIA01	Piano di gestione degli incidenti di sicurezza IT	Gestione degli eventi e degli incidenti di sicurezza
REGP_PIA02	Piano di gestione delle vulnerabilità	Identificazione, valutazione, trattamento e monitoraggio delle vulnerabilità
REGP_PIA03	Valutazione del rischio cyber	Identificazione, analisi e ponderazione dei rischi
REGP_PIA04	Piano di trattamento dei rischi per la sicurezza informatica	Decisioni e misure di trattamento dei rischi
REGP_PIA05	Piano di adeguamento NIS2	Pianificazione e monitoraggio degli interventi di adeguamento
REGP_PIA06	Piano di formazione in materia di sicurezza informatica	Formazione e consapevolezza
REGP_PIA07	Piano di continuità operativa	Continuità dei servizi e delle attività
REGP_PIA08	Piano di disaster recovery	Ripristino dei sistemi e dei servizi in caso di disastro
REGP_PIA09	Piano di gestione della crisi cyber	Coordinamento e gestione delle situazioni di crisi
REGP_PR01	Procedure per la sicurezza informatica	Procedure operative di attuazione delle politiche e dei piani
REGP_INV01	Mappa delle fonti inventariali degli asset	Fonti e strumenti utilizzati per il censimento degli asset

I piani, le procedure e le istruzioni operative collegate alla presente Politica riportano, ove necessario, i riferimenti specifici applicabili al rispettivo ambito di disciplina.