Codice A1600A
D.D. 30 marzo 2026, n. 209
D.Lgs. 4 settembre 2024 n. 138. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica. Presa d'atto del ''Piano di Gestione degli Incidenti di Sicurezza IT''.

ATTO DD 209/A1600A/2026 DEL 30/03/2026

DETERMINAZIONE DIRIGENZIALE
A1600A - AMBIENTE, ENERGIA E TERRITORIO

OGGETTO: D.Lgs. 4 settembre 2024 n. 138. Disposizioni per adempiere agli obblighi in materia di sicurezza informatica. Presa d'atto del "Piano di Gestione degli Incidenti di Sicurezza IT"

Premesso che:

La Direttiva (UE) 2022/2555 (NIS2) 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 recepisce la direttiva (UE) 2022/2555, 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 medesimo decreto legislativo 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 D.Lgs. 4 settembre 2024 n. 138 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’art. 7, comma 1, lettera c), del D. Lgs. 4 settembre 2024 n. 138 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 a Regione Piemonte in virtù del disposto dell’art. 3 comma 6 e dell’allegato III del decreto legislativo stesso;

Regione Piemonte è un Ente considerato “soggetto importante” ai fini dell’applicazione della normativa di riferimento per le ragioni di cui in premessa;

gli obblighi di segnalazione incidenti di sicurezza informatica, derivanti dalla Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio e recepiti in Italia dal D. Lgs. 138/2024, diventano operativi per i soggetti Essenziali e per i soggetti Importanti a partire dal 1° gennaio 2026, con tempistiche di notifica che prevedono un preallarme entro 24 ore (ove l'incidente sia significativo) e la notifica completa entro 72 ore dalla scoperta, una volta che l'organizzazione è stata inserita nell'elenco ACN.

Per ottemperare a tale obbligo il Referente per la Cybersicurezza di Regione Piemonte ha predisposto un Piano di Gestione degli Incidenti di Sicurezza IT, che 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.

Gli obiettivi del Piano sono di 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.

Gli organi amministrativi di vertice, così come individuati dal decreto legislativo 138/2024, hanno validato il Piano nella seduta del Comitato di Coordinamento Direttori in data 16 dicembre 2025;

Ritenuto opportuno, per quanto sopra esposto:
prevedere le misure tecniche, operative e organizzative finalizzate alla gestione dei rischi posti alla sicurezza dei sistemi informativi di competenza della Direzione, nonché a prevenire o ridurre al minimo l'impatto degli incidenti adottando il “Piano di Gestione degli Incidenti di Sicurezza IT” approvato dal Coordinamento Direttori, contenente le misure sopra richiamate;

attivare, con l’impegno dei referenti della Cybersicurezza nominati per la Direzione, le attività di competenza della direzione affidandone il coordinamento al Responsabile del Settore Sistema informativo territoriale e ambientale per renderle più efficaci tra il personale dei Settori;

dare effettiva attuazione al Piano di Gestione degli Incidenti di Sicurezza IT, mantenendo, attraverso il Responsabile del Settore Sistema informativo territoriale e ambientale ed i referenti della Cybersicurezza nominati per la Direzione, un costante rapporto con il Referente per la Cybersicurezza dell’Ente in merito alle attività e le responsabilità che il Piano stesso demanda alle Direzioni regionali.

Attestata la regolarità amministrativa del presente provvedimento ai sensi della D.G.R. 25 gennaio 2024 n. 8-8111

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";
- La Direttiva (UE) 2022/2555 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;
- a Legge 90 del 2024 " Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici";
- 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,;
- 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 Direttiva 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";

determina

per le motivazioni evidenziate in premessa:

- di prendere atto del "Piano di Gestione degli Incidenti di Sicurezza IT", così come validato dagli organi amministrativi e direttivi, identificati in base all'art. 23 del "Decreto NIS 2", di cui all'Allegato 1, parte integrante e sostanziale del presente provvedimento;

- di prevedere le misure tecniche, operative e organizzative finalizzate alla gestione dei rischi posti alla sicurezza dei sistemi informativi di competenza della Direzione, nonché a prevenire o ridurre al minimo l'impatto degli incidenti adottando il "Piano di Gestione degli Incidenti di Sicurezza IT" approvato dal Coordinamento Direttori, contenente le misure sopra richiamate;

- di attivare, con l'impegno dei referenti della Cybersicurezza nominati per la Direzione, le attività di competenza della direzione affidandone il coordinamento al Responsabile del Settore Sistema informativo territoriale e ambientale per renderle più efficaci tra il personale dei Settori;

- di dare effettiva attuazione al Piano di Gestione degli Incidenti di Sicurezza IT, mantenendo, attraverso il Responsabile del Settore Sistema informativo territoriale e ambientale ed i referenti della Cybersicurezza nominati per la Direzione, un costante rapporto con il Referente per la Cybersicurezza dell'Ente in merito alle attività e le responsabilità che il Piano stesso demanda alle Direzioni regionali.

La presente determinazione non è soggetta alla pubblicazione ai sensi del Decreto Legislativo 33/2013, nella sezione "Amministrazione trasparente" del sito istituzionale della Regione Piemonte.

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 (A1600A - AMBIENTE, ENERGIA E TERRITORIO)
Firmato digitalmente da Angelo Robotto

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 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

1. regp-pia01-piano-gestione-incidenti-sicurezza-it-def.pdf Allegato

VERIFICHE ED APPROVAZIONI

VER.	REDAZIONE		CONTROLLO ED APPROVAZIONE	
	NOME	DATA	NOME	DATA
V01	Settore Sistema Informativo	Novembre 2025	Coordinamento Direttori	16/12/2025

STATO DELLE VARIAZIONI

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

INDICE

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 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 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 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.

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 1a

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

2 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.

2.1 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.

2.2 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 RS.MA-01 punto 1c

2.3 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.

2.4 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.

2.5 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].

2.6 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 RC.RP-01 punto 1

2.7 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	Coordinamento Direttori

			Regionale, Settore Servizi Infrastrutturali e 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.

3 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]

4 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

8 Requisito NIS2 DE.CM-01 punto 2

9 Requisito NIS2 RS.MA-01 punto 1b

l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

- 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.

5 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.MA-01 punto 1e
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.

5.1 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.

5.2 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.

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,

12 Requisito NIS2 RS.CO-02 punto 1

13 Requisito NIS2 RS.MA-01 punto 1d

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).

6 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 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..).

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

14 Requisito NIS2 RS.CO-02 punto 2

- 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 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.