MANUALE OPERATIVO DI SEGNALAZIONE E GESTIONE DEGLI INCIDENTI INFORMATICI

Versione:	1.0
Anno:	2026
Approvazione	Comitato di Indirizzo – deliberazione n. 17 del 12 maggio 2026
Responsabile:	Responsabile Transizione Digitale RTD
Referente	Referente Cybersicurezza

Sommario

GLOSSARIO

Il presente glossario raccoglie i principali termini tecnici, organizzativi e normativi richiamati nel Manuale operativo di segnalazione e gestione degli incidenti informatici. Le definizioni sono coerenti con il quadro normativo applicabile — in particolare D.Lgs. 138/2024 (recepimento NIS2), L. 90/2024, Determinazione ACN n. 164179/2025, Regolamento (UE) 2016/679 (GDPR) e D.Lgs. 82/2005 (CAD) — e con le linee guida AgID e ACN. Le voci sono ordinate alfabeticamente.

Termine	Definizione
ACN — Agenzia per la Cybersicurezza Nazionale	Autorità nazionale, istituita con D.L. 14 giugno 2021, n. 82, competente in materia di cybersicurezza per la tutela degli interessi nazionali nel settore. Per AIPo costituisce l'Autorità competente NIS e il punto di contatto unico per la notifica degli incidenti informatici significativi ai sensi del D.Lgs. 138/2024.
AgID — Agenzia per l'Italia Digitale	Agenzia tecnica della Presidenza del Consiglio dei Ministri che emana linee guida e regole tecniche in materia di digitalizzazione della Pubblica Amministrazione, ivi comprese le Misure Minime di Sicurezza ICT richiamate dal Manuale.
Aggiornamento successivo (notifica)	Comunicazione integrativa che AIPo trasmette all'ACN dopo la notifica iniziale, per rappresentare l'evoluzione dell'incidente, l'esito delle misure di contenimento e mitigazione, lo stato di ripristino dei sistemi e ogni ulteriore impatto emerso.
Amministratore di sistema	Figura tecnica, individuata ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i., che svolge attività di gestione, configurazione e manutenzione dei sistemi informativi dell'Ente. Nel ciclo di vita dell'incidente esegue, sotto il coordinamento del Referente per la cybersicurezza, le operazioni di analisi tecnica, contenimento, mitigazione e ripristino.
Analisi forense (digital forensics)	Insieme delle attività tecniche di acquisizione, conservazione, analisi e documentazione delle evidenze digitali, condotte con modalità tali da preservarne integrità e valore probatorio. Riferita nel Manuale alla conservazione delle evidenze tecniche (par. 10.5).
Analisi preliminare	Prima fase tecnica del processo di gestione dell'incidente, finalizzata ad acquisire una comprensione iniziale dell'evento (natura, estensione, sistemi coinvolti) sulla base delle informazioni del segnalante, dei dati tecnici e dei log disponibili. È condotta dalla struttura ICT sotto il coordinamento del Referente per la cybersicurezza.
Approccio prudenziale	Criterio di valutazione che, in caso di incertezza sulla significatività di un incidente o sulla sussistenza dei presupposti per la notifica, privilegia la notifica e l'attivazione delle procedure rispetto all'omissione.
Autenticità	Proprietà di un dato, di un sistema o di una comunicazione di poter essere ricondotti con certezza al soggetto da cui dichiarano di provenire. Insieme a riservatezza, integrità e disponibilità costituisce uno dei requisiti la cui compromissione configura un incidente informatico (par. 3.1).

Backup	Copia di sicurezza di dati, configurazioni o sistemi, conservata su supporto separato e utilizzabile per il ripristino in caso di indisponibilità, alterazione o perdita degli originali. Strumento essenziale per il ripristino dei servizi (par. 6.11) e per la continuità operativa.
CAD — Codice dell'Amministrazione Digitale	D.Lgs. 7 marzo 2005, n. 82 e s.m.i., che disciplina l'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, anche con riferimento alla sicurezza informatica e alla continuità operativa.
Catena di custodia	Sequenza documentata dei passaggi di possesso, conservazione e analisi di un'evidenza digitale, finalizzata a dimostrarne autenticità e integrità. Garantisce l'utilizzabilità delle evidenze in sede ispettiva, giudiziaria o di indagine interna.
Chiusura formale dell'incidente	Atto con cui il Referente per la cybersicurezza dichiara conclusa la gestione operativa dell'incidente, dopo aver verificato il ripristino in condizioni di sicurezza dei sistemi e dei servizi, l'adozione delle principali misure di mitigazione e la conclusione delle attività di notifica (par. 9.2). Non preclude le ulteriori attività di analisi della fase post-incidente.
Classificazione dell'incidente	Attribuzione dell'incidente a una o più categorie di impatto — riservatezza, integrità, disponibilità, incidenti combinati — secondo i criteri del par. 3.4 del Manuale, ai fini del coordinamento delle attività di gestione e dell'attivazione delle procedure di notifica.
Compromissione	Condizione in cui la riservatezza, l'integrità, la disponibilità o l'autenticità di un dato, di un sistema o di un servizio risulta violata, alterata o messa a rischio.
Contenimento	Insieme delle misure immediate volte a circoscrivere l'incidente, impedirne la propagazione e limitarne l'impatto sui sistemi e sui servizi dell'Ente. Può comportare, a titolo esemplificativo, l'isolamento di sistemi o reti, la sospensione temporanea di servizi, la revoca di credenziali (par. 6.9).
Continuità operativa (Business Continuity)	Capacità dell'Ente di mantenere la fornitura dei servizi essenziali, o di ripristinarli entro tempi accettabili, anche in presenza di eventi avversi. È coordinata con la gestione degli incidenti quando l'evento ha impatto rilevante sull'operatività (par. 6.12).
CSI Piemonte	Soggetto in house pluripartecipato, di cui AIPo si avvale per la gestione di una parte significativa dei sistemi applicativi e dei servizi gestiti in ambiente cloud. Opera nel ciclo di vita dell'incidente su attivazione del Referente per la cybersicurezza, nell'ambito delle proprie competenze tecniche, senza acquisire la responsabilità complessiva del processo (par. 4.6).
CSIRT Italia	Computer Security Incident Response Team nazionale, struttura operante presso l'ACN competente per la ricezione delle notifiche di incidente, per il coordinamento della risposta a livello nazionale e per la diffusione di alert e indicatori di compromissione.
Cybersicurezza (Cybersecurity)	Insieme delle attività organizzative, tecniche e procedurali finalizzate alla protezione della disponibilità, dell'integrità, della riservatezza e

	dell'autenticità di reti, sistemi informativi, dati e servizi digitali, dalla minaccia di eventi accidentali o dolosi.
Data breach (violazione di dati personali)	Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali (art. 4, n. 12, GDPR). In presenza di data breach AIPo, tramite RPD, attiva le valutazioni ai sensi degli artt. 33 e 34 GDPR e, ove richiesto, la notifica al Garante.
Determinazione ACN n. 164179/2025	Atto dell'Agenzia per la Cybersicurezza Nazionale che definisce le misure di sicurezza applicabili ai soggetti NIS Importanti, integrando il D.Lgs. 138/2024 sul piano tecnico e organizzativo. Costituisce uno dei principali riferimenti del Manuale (par. 2.2).
Direttiva NIS2 (Direttiva UE 2022/2555)	Direttiva del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recepita in Italia dal D.Lgs. 138/2024.
Disponibilità	Proprietà di un dato, di un sistema o di un servizio di essere accessibile e utilizzabile, su richiesta dei soggetti autorizzati, nei tempi e nei modi previsti.
D.Lgs. 138/2024	Decreto legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva UE 2022/2555 (NIS2). Disciplina obblighi organizzativi, di gestione del rischio e di notifica degli incidenti per i soggetti essenziali e importanti, definendo, all'art. 24, le tempistiche di preallarme (24 ore), notifica iniziale (72 ore) e relazione finale (un mese).
Eradicazione	Fase del ciclo di gestione dell'incidente in cui sono rimosse le cause e le componenti malevole presenti nei sistemi (es. malware, account compromessi, regole di firewall alterate). Nel Manuale è ricompresa nelle attività di mitigazione (par. 6.10).
Escalation	Procedura di innalzamento progressivo del livello di coinvolgimento delle figure decisionali, in funzione della gravità e dell'impatto dell'evento. Nel Manuale è coordinata dal Referente per la cybersicurezza (par. 4.8).
Esfiltrazione di dati	Trasferimento non autorizzato di dati dall'interno dei sistemi dell'Ente verso destinazioni esterne. Configura un incidente informatico tipico, con possibile impatto su riservatezza e — se riguarda dati personali — qualifica un data breach.
Evento di sicurezza	Qualsiasi evento osservabile o segnalazione relativa alla sicurezza dei sistemi informativi che non abbia ancora prodotto un impatto negativo accertato, ma che richiede monitoraggio e valutazione (par. 3.2). Si distingue dall'incidente informatico per l'assenza di impatto effettivo.
Evidenza	Informazione, registrazione o supporto, di natura tecnica, organizzativa o documentale, che documenta l'occorrenza, le caratteristiche o la gestione di un incidente. Le evidenze sono oggetto di conservazione strutturata (Capitolo 10).
Fornitore	Soggetto esterno all'Ente che, in forza di un rapporto contrattuale, eroga prodotti o servizi che possono interessare i sistemi informativi dell'AIPo. La gestione di incidenti che coinvolgono fornitori richiede il coordinamento con il Referente per la cybersicurezza (par. 7.13).

Garante per la protezione dei dati personali	Autorità amministrativa indipendente competente per la tutela dei dati personali. È destinataria della notifica del data breach ai sensi dell'art. 33 GDPR, ove ne ricorrano i presupposti.
GDPR — Regolamento (UE) 2016/679	Regolamento generale sulla protezione dei dati. Disciplina, fra l'altro, gli obblighi di notifica all'Autorità di controllo (art. 33) e di comunicazione agli interessati (art. 34) in caso di violazione di dati personali.
Gestione del rischio ICT	Processo strutturato di identificazione, analisi, valutazione e trattamento dei rischi che gravano sui sistemi informativi e sui servizi digitali dell'Ente, anche al fine di definire le misure di sicurezza e di continuità operativa.
Governance della sicurezza	Sistema dei principi, delle responsabilità e dei flussi decisionali con cui l'Ente indirizza, coordina e controlla il proprio modello di sicurezza informatica. Improntata ai principi di unitarietà, coordinamento, responsabilità e tracciabilità (par. 4.1).
Hardening	Insieme di interventi tecnici di rafforzamento delle configurazioni di sicurezza di sistemi, applicazioni e dispositivi, finalizzati a ridurre la superficie di attacco. Tipico esempio di azione correttiva post-incidente.
Helpdesk ICT	Servizio interno di supporto agli utenti per la segnalazione e la gestione di problemi informatici. Costituisce uno dei canali primari di segnalazione interna degli incidenti (helpdesk@agenziapo.it, par. 5.9).
In house (soggetto)	Soggetto giuridico, partecipato dall'Ente o da un insieme di amministrazioni, che eroga servizi informatici nei confronti dei propri soci secondo il modello di affidamento in house providing. Per AIPo: CSI Piemonte e Lepida (par. 4.6).
Incidente informatico	Qualsiasi evento, singolo o ripetuto, che abbia compromesso o possa compromettere la disponibilità, l'integrità, la riservatezza o l'autenticità di dati, sistemi, reti o servizi informatici dell'Ente, causando o potendo causare un impatto negativo sull'operatività (par. 3.1).
Incidente significativo	Incidente informatico che, per natura, estensione o impatto, determina conseguenze rilevanti per l'operatività dell'Ente o per i soggetti interessati e che può richiedere l'attivazione di procedure di notifica verso l'esterno (par. 3.3). I criteri di significatività sono coerenti con il D.Lgs. 138/2024.
Indicatore di compromissione (IoC)	Elemento tecnico osservabile (indirizzi IP, hash di file, domini, pattern nei log) la cui presenza fa ritenere probabile la compromissione di un sistema. È oggetto di scambio informativo con CSIRT Italia.
Integrità	Proprietà di un dato, di un sistema o di un servizio di non subire alterazioni non autorizzate, accidentali o dolose, e di poter essere modificato esclusivamente con modalità controllate.
L. 90/2024	Legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. Prevede, fra l'altro, l'obbligo per le PA di individuare una struttura per la cybersicurezza e di designare un Referente per la cybersicurezza (art. 8).

Lepida	Società in house della Regione Emilia-Romagna e degli enti pubblici dell'area regionale, che fornisce ad AIPo servizi relativi all'infrastruttura di rete e all'ospitalità dei sistemi in ambiente cloud certificato (par. 4.6).
Lessons learned	Insieme delle conclusioni operative e organizzative tratte dall'analisi post-incidente, utilizzate per orientare le azioni correttive, gli aggiornamenti documentali e le iniziative di formazione (Capitolo 9).
Log (registro)	Registrazione cronologica e automatica di eventi prodotta da sistemi, applicazioni e dispositivi di rete. Costituisce evidenza tecnica primaria per la rilevazione, l'analisi e la ricostruzione degli incidenti.
Malware	Programma o codice informatico progettato per danneggiare un sistema, sottrarre informazioni o compromettere il funzionamento di reti e servizi. Comprende, a titolo esemplificativo, virus, worm, trojan, spyware e ransomware.
Mitigazione	Insieme delle misure tecniche e organizzative volte a ridurre l'impatto residuo dell'incidente e a rimuovere, ove possibile, le cause e le vulnerabilità che ne hanno consentito o favorito il verificarsi (par. 6.10).
MFA — Autenticazione a più fattori	Meccanismo di autenticazione che richiede la combinazione di più fattori indipendenti (qualcosa che si conosce, si possiede, si è) per il riconoscimento dell'utente. Misura tipica di rafforzamento adottata in ambito incident response.
Misure Minime di Sicurezza ICT (AgID)	Insieme di controlli di sicurezza, di matrice AgID, che le pubbliche amministrazioni sono tenute ad applicare per assicurare un livello di base di protezione dei sistemi informativi. Costituiscono riferimento documentale del Manuale (par. 2.3).
Need-to-know (necessità di conoscere)	Principio per cui le informazioni sono condivise esclusivamente con i soggetti che, in relazione al ruolo ricoperto, necessitano di accedervi ai fini della gestione dell'incidente o degli adempimenti normativi (par. 8.2).
Notifica iniziale	Comunicazione che AIPo trasmette all'ACN entro 72 ore dalla presa di consapevolezza dell'incidente significativo, per fornire una prima informazione sull'evento, sulle caratteristiche principali, sui sistemi e servizi interessati e sulle misure già adottate (par. 7.7-7.8).
Organi di vertice	Organi di indirizzo e di governo dell'AIPo, cui la normativa attribuisce la responsabilità ultima in materia di sicurezza informatica e gestione degli incidenti. Approvano il Manuale, sono informati sugli incidenti rilevanti e assumono le decisioni strategiche (par. 4.3).
Patch	Aggiornamento software volto a correggere vulnerabilità, errori o malfunzionamenti. L'applicazione tempestiva delle patch costituisce misura preventiva e correttiva frequente nella gestione degli incidenti.
Perimetro di sicurezza nazionale cibernetica	Quadro normativo di tutela rafforzata, istituito con D.L. 105/2019, applicabile ai soggetti che svolgono funzioni essenziali dello Stato o erogano servizi essenziali. Pur non essendo AIPo direttamente inclusa, il Manuale ne tiene conto per le parti applicabili (par. 2.2).
Phishing	Tecnica di ingegneria sociale, tipicamente veicolata via posta elettronica o messaggistica, finalizzata a indurre l'utente a fornire credenziali o dati sensibili o ad aprire allegati e collegamenti malevoli.

Post-incidente	Fase successiva alla chiusura formale dell'incidente, dedicata all'analisi delle cause, alla valutazione dell'efficacia delle misure adottate e all'individuazione delle azioni correttive di miglioramento continuo (Capitolo 9).
Preallarme (early warning)	Comunicazione che AIPo trasmette all'ACN entro 24 ore dalla presa di consapevolezza di un incidente potenzialmente significativo, per attivare tempestivamente il sistema di supporto nazionale, anche in assenza di una valutazione completa dell'evento (art. 24, D.Lgs. 138/2024).
Presa in carico	Atto formale con cui il Referente per la cybersicurezza assume il coordinamento operativo dell'incidente, attivando le strutture coinvolte e dando avvio all'analisi preliminare (par. 6.3).
Quasi-incidente (near miss)	Evento che, pur non avendo prodotto danni accertati, presenta caratteristiche tali da far ritenere probabile un impatto negativo sui sistemi o sui dati e che, ai fini del Manuale, è ricompreso nella nozione di incidente informatico (par. 3.1).
Ransomware	Tipologia di malware che cifra i dati o blocca l'accesso ai sistemi, richiedendo il pagamento di un riscatto per il ripristino. Configura un incidente informatico tipicamente significativo per l'impatto su disponibilità e integrità dei dati.
Referente per la cybersicurezza	Figura individuata ai sensi dell'art. 8 della L. 90/2024 e nominata da AIPo, che coordina operativamente il processo di gestione degli incidenti, mantiene il registro degli incidenti, valuta l'attivazione delle procedure di notifica ed è il punto di contatto unico dell'Ente con l'ACN (par. 4.4).
Registro degli incidenti informatici	Repertorio interno tenuto dal Referente per la cybersicurezza, in cui sono annotati gli incidenti gestiti dall'Ente, le notifiche effettuate, le evidenze conservate e gli esiti delle valutazioni post-incidente.
Relazione finale	Comunicazione conclusiva che AIPo trasmette all'ACN entro un mese dalla notifica iniziale, contenente il quadro complessivo dell'incidente, delle cause individuate, delle misure adottate e degli esiti delle attività di ripristino e miglioramento (art. 24, D.Lgs. 138/2024; par. 7.10).
Resilienza	Capacità dell'Ente e dei suoi sistemi informativi di prevenire, resistere, rispondere e recuperare dagli incidenti, mantenendo la continuità dei servizi essenziali. Obiettivo primario del quadro normativo NIS2.
Responsabile della Protezione dei Dati (RPD/DPO)	Figura prevista dagli artt. 37-39 del GDPR, designata dal Titolare del trattamento per vigilare sull'osservanza della normativa sulla protezione dei dati. Coinvolto nei casi in cui l'incidente comporti o possa comportare una violazione di dati personali (par. 4.7).
Riservatezza	Proprietà di un dato o di un'informazione di non essere resa accessibile o divulgata a soggetti non autorizzati.
Ripristino (recovery)	Fase di ricostituzione delle condizioni operative ordinarie, conclusa la quale i sistemi e i servizi possono essere reimmessi in produzione previa verifica delle condizioni di sicurezza (par. 6.11).
RTD — Responsabile per la Transizione Digitale	Figura prevista dall'art. 17 del CAD, responsabile della transizione alla modalità operativa digitale dell'amministrazione. Per AIPo è coinvolto

	nel coordinamento delle attività di revisione e aggiornamento del Manuale (par. 11.4).
Segnalante	Soggetto, interno o esterno, che rileva un evento sospetto o un incidente e lo comunica attraverso i canali ufficiali. La sua responsabilità si esaurisce nella tempestiva comunicazione di quanto osservato, senza interpretazioni tecniche (par. 5.7).
Segnalazione interna	Comunicazione tempestiva, effettuata dal segnalante attraverso i canali ufficiali (helpdesk@agenziapo.it, cybersicurezza@agenziapo.it), di un evento o anomalia potenzialmente riconducibile a un incidente informatico (Capitolo 5).
SIEM — Security Information and Event Management	Soluzione tecnologica che raccoglie, correla e analizza in modo centralizzato i log provenienti da sistemi e dispositivi di sicurezza, supportando le attività di rilevazione, analisi e risposta agli incidenti.
Soggetti NIS Importanti / Essenziali	Categorie di soggetti, definite dal D.Lgs. 138/2024 sulla base dei settori e della dimensione, soggetti agli obblighi di gestione del rischio e di notifica degli incidenti previsti dalla NIS2. AIPo, in qualità di soggetto NIS Importante, applica le misure di cui alla Determinazione ACN 164179/2025.
Tempistiche di notifica	Termini fissati dall'art. 24 del D.Lgs. 138/2024 per la comunicazione all'ACN degli incidenti significativi: preallarme entro 24 ore, notifica iniziale entro 72 ore, relazione finale entro un mese, decorrenti dal momento di acquisita ragionevole consapevolezza dell'evento.
Ticketing (sistema di)	Strumento informatico di registrazione e gestione delle richieste di assistenza, utilizzato come canale primario di segnalazione interna degli eventi e degli incidenti informatici (par. 5.9).
Tracciabilità	Caratteristica del processo che consente di ricostruire, in modo cronologico e verificabile, le attività svolte, le decisioni assunte, i soggetti coinvolti e i tempi di esecuzione. Principio fondante della governance della gestione degli incidenti (par. 4.1).
Triage	Attività di valutazione iniziale rapida finalizzata a stabilire la priorità di trattamento dell'evento segnalato e a indirizzarlo alle strutture competenti. Corrisponde, nel Manuale, alle attività di presa in carico e analisi preliminare.
Valutazione di gravità	Apprezzamento complessivo dell'impatto dell'incidente, basato sugli indicatori del par. 3.5 (sistemi coinvolti, utenti impattati, durata dell'indisponibilità, criticità dei dati, conseguenze legali ed economiche, capacità di propagazione). Costituisce la base per le decisioni di escalation e di notifica.
Vulnerabilità	Debolezza tecnica, organizzativa o procedurale di un sistema, di un'applicazione o di un processo che può essere sfruttata, accidentalmente o intenzionalmente, per produrre un impatto negativo sulla sicurezza.

CAPITOLO 1 – PREMESSA E FINALITÀ

1.1 Premessa

Il presente Manuale di segnalazione e gestione degli incidenti informatici disciplina l'insieme delle modalità organizzative e procedurali adottate dall'Agenzia Interregionale per il fiume Po (AIPo) per la segnalazione, la gestione e il trattamento degli incidenti informatici che possano incidere sui sistemi informativi, sulle reti, sui servizi digitali e sui dati trattati dall'Ente.

Il Manuale è adottato in attuazione della normativa vigente in materia di cybersicurezza e resilienza digitale e si inserisce nel quadro delle misure organizzative e tecniche finalizzate a garantire la continuità operativa, la sicurezza delle informazioni e l'affidabilità dei servizi istituzionali.

La crescente dipendenza delle attività amministrative da strumenti e infrastrutture digitali rende necessario disporre di procedure formalizzate che consentano di affrontare in modo strutturato, tempestivo e documentabile gli eventi che possano compromettere la sicurezza informatica dell'Ente.

1.2 Oggetto del Manuale

Il presente Manuale ha ad oggetto la definizione delle regole e delle procedure interne relative:

- alla segnalazione di eventi, anomalie e incidenti informatici;
- alla gestione operativa degli incidenti informatici;
- alla classificazione degli incidenti e alla valutazione della loro gravità;
- all'individuazione dei ruoli e delle responsabilità coinvolti;
- alla tracciabilità e alla documentazione delle attività svolte.

Il Manuale costituisce riferimento procedurale per tutto il personale dell'AIPo, nonché per i soggetti esterni che, a qualsiasi titolo, operano sui sistemi informativi dell'Ente.

1.3 Finalità

La finalità del presente Manuale è quella di assicurare che la gestione degli incidenti informatici avvenga secondo criteri di uniformità, proporzionalità e responsabilità, riducendo il rischio di decisioni estemporanee o non coordinate.

In particolare, il Manuale è finalizzato a:

- garantire la tempestiva individuazione e segnalazione degli incidenti informatici;
- assicurare una gestione coordinata e documentata degli eventi;
- limitare l'impatto degli incidenti sui servizi, sui dati e sull'operatività dell'Ente;
- assicurare il rispetto degli obblighi normativi in materia di comunicazione e notifica;
- fornire evidenza delle misure organizzative adottate dall'Ente in materia di cybersicurezza.

Il Manuale contribuisce inoltre a rafforzare la consapevolezza del personale in merito al proprio ruolo nella tutela della sicurezza informatica dell'Ente.

1.4 Ambito di applicazione soggettivo e oggettivo

Le disposizioni del presente Manuale si applicano a tutti i sistemi informativi, alle infrastrutture digitali, alle reti e ai servizi informatici utilizzati dall'AIPo per lo svolgimento delle proprie funzioni istituzionali.

Il Manuale si applica a tutto il personale dell'Ente, indipendentemente dalla qualifica o dal ruolo ricoperto, nonché ai collaboratori, consulenti e fornitori che, sulla base di specifici rapporti contrattuali o convenzionali, accedono ai sistemi informativi dell'AIPo.

Le procedure disciplinate dal Manuale trovano applicazione sia in presenza di incidenti informatici già manifestatisi, sia in relazione a eventi o anomalie che possano ragionevolmente prefigurare il verificarsi di un incidente.

1.5 Inquadramento del Manuale nel sistema di governance dell'Ente

Il presente Manuale costituisce parte integrante del sistema di governance della sicurezza informatica dell'AIPo ed è coordinato con le politiche, i piani e gli atti organizzativi adottati dall'Ente in materia di gestione dei sistemi informativi, protezione dei dati e continuità operativa.

Il Manuale assume valore di documento ufficiale dell'Ente e rappresenta riferimento procedurale sia per le attività interne sia ai fini di eventuali controlli, verifiche o ispezioni da parte delle autorità competenti.

Il Manuale è soggetto a revisione periodica, nonché ad aggiornamento in caso di modifiche normative, evoluzioni organizzative o tecnologiche rilevanti, ovvero a seguito della gestione di incidenti informatici significativi.

CAPITOLO 2 – RIFERIMENTI NORMATIVI E DOCUMENTALI

2.1 Quadro normativo di riferimento

Il presente Manuale è redatto in conformità al quadro normativo nazionale ed europeo vigente in materia di cybersicurezza, resilienza digitale e gestione degli incidenti informatici, con particolare riferimento alle disposizioni applicabili alle pubbliche amministrazioni e agli enti pubblici.

Le procedure e le misure organizzative disciplinate nel Manuale trovano fondamento nelle disposizioni che impongono alle amministrazioni pubbliche l'adozione di assetti organizzativi e procedurali idonei a prevenire, rilevare e gestire incidenti informatici, nonché a garantire la continuità operativa e la sicurezza delle informazioni. Il Manuale recepisce inoltre i principi di responsabilità, proporzionalità, tracciabilità e documentazione delle attività, che costituiscono elementi essenziali ai fini della verifica dell'adeguatezza delle misure adottate dall'Ente.

2.2 Normativa applicabile

Il presente Manuale è adottato in attuazione e nel rispetto della normativa nazionale in materia di rafforzamento della cybersicurezza e di prevenzione e contrasto dei reati informatici, nonché della normativa di recepimento della Direttiva (UE) 2022/2555 (NIS2), che disciplina le misure volte a garantire un livello comune elevato di cybersicurezza. In particolare si fa riferimento a: D.Lgs. 4 settembre 2024, n. 138; L. 28 giugno 2024, n. 90; Determinazione ACN n. 164179/2025 (misure di sicurezza per soggetti NIS Importanti).

Tale quadro normativo definisce obblighi specifici in capo agli enti pubblici in relazione alla gestione del rischio informatico, all'organizzazione delle funzioni di cybersicurezza, alla gestione e alla segnalazione degli incidenti, nonché alla responsabilità degli organi di vertice. Per quanto applicabile, il Manuale tiene conto anche delle disposizioni in materia di perimetro di sicurezza nazionale cibernetica.

Le procedure descritte nel presente Manuale sono interpretate e applicate in coerenza con l'evoluzione del quadro normativo di riferimento.

2.3 Linee guida e atti di indirizzo

Il Manuale tiene conto delle linee guida, delle determinazioni e degli atti di indirizzo emanati dalle autorità competenti in materia di cybersicurezza, con particolare riferimento alle indicazioni operative in tema di rafforzamento della resilienza informatica, gestione degli incidenti, individuazione dei ruoli e delle responsabilità, nonché documentazione e conservazione delle evidenze.

Le disposizioni del presente Manuale sono da intendersi dinamicamente allineate agli aggiornamenti delle linee guida e degli atti di indirizzo adottati successivamente alla sua approvazione, nei limiti della loro compatibilità con l'organizzazione e le attività dell'Agenzia Interregionale per il fiume Po (AIPo).

2.4 Documentazione interna di riferimento

Il presente Manuale si inserisce nel sistema documentale dell'AIPo e deve essere applicato in coordinamento con gli altri atti e documenti interni adottati dall'Ente in materia di sicurezza informatica, protezione dei dati e governance ICT.

In particolare, il Manuale è coordinato con i documenti di pianificazione in ambito ICT, con le politiche di sicurezza informatica, con il Piano per la sicurezza informatica e gestione del rischio ICT di AIPo, con la documentazione relativa al trattamento dei dati personali e con i piani di continuità operativa adottati dall'Ente.

Tali documenti concorrono a definire il contesto organizzativo entro il quale si applicano le procedure del presente Manuale e devono essere consultati unitamente ad esso.

2.5 Valore del Manuale ai fini organizzativi e ispettivi

Il presente Manuale costituisce documento ufficiale dell'AIPo e rappresenta evidenza dell'adozione di misure organizzative adeguate in materia di gestione degli incidenti informatici.

Esso assume rilievo sia quale riferimento operativo per il personale dell'Ente sia quale strumento di dimostrazione della conformità alle disposizioni normative applicabili, nei confronti delle autorità di vigilanza e controllo, ivi inclusa l'Agenzia per la Cybersicurezza Nazionale (ACN).

CAPITOLO 3 – DEFINIZIONI E CLASSIFICAZIONE DEGLI INCIDENTI

3.1 Definizione di incidente informatico

Ai fini del presente Manuale, per incidente informatico si intende qualsiasi evento, singolo o ripetuto, che abbia compromesso o possa compromettere la disponibilità, l'integrità, la riservatezza o l'autenticità di dati, sistemi, reti o servizi informatici dell'Ente, causando o potendo causare un impatto negativo sull'operatività dell'AIPo.

Un incidente informatico può derivare da:

- azioni dolose (attacchi informatici, accessi non autorizzati, malware);
- eventi accidentali (errori umani, guasti hardware o software);
- cause esterne o ambientali che incidono sul funzionamento dei sistemi.

Sono ricompresi nella definizione di incidente informatico anche gli eventi che, pur non avendo prodotto danni accertati, presentino caratteristiche tali da far ritenere probabile un impatto negativo sui sistemi o sui dati dell'Ente.

3.2 Distinzione tra evento di sicurezza e incidente informatico

Ai fini della corretta gestione operativa, si distingue tra:

a) Evento di sicurezza

Qualsiasi evento osservabile o segnalazione relativa alla sicurezza dei sistemi informativi che non abbia ancora prodotto un impatto negativo accertato, ma che richiede monitoraggio e valutazione. Rientrano in questa categoria, a titolo esemplificativo:

- anomalie nei log di sistema;
- tentativi di accesso falliti ripetuti;
- alert di sicurezza o segnalazioni preventive.

b) Incidente informatico

Evento o insieme di eventi che ha prodotto o può produrre un impatto negativo sulla disponibilità, l'integrità o la riservatezza dei sistemi o dei dati dell'Ente e che richiede l'attivazione delle procedure di gestione previste dal presente Manuale.

3.3 Incidente informatico significativo

Un incidente informatico significativo è un incidente che, per natura, estensione o impatto, determina conseguenze rilevanti per l'operatività dell'Ente o per i soggetti interessati, e che può richiedere l'attivazione di procedure di notifica verso l'esterno.

Ai fini del presente Manuale, un incidente è considerato significativo quando ricorre almeno una delle seguenti condizioni:

- provoca o può provocare una interruzione grave o un degrado rilevante dei servizi informatici o digitali dell'Ente;
- comporta un danno materiale o immateriale rilevante, inclusi danni economici, reputazionali o organizzativi;
- coinvolge un numero elevato di utenti, sistemi o dati, oppure sistemi critici per le attività istituzionali;
- determina una compromissione della riservatezza o dell'integrità di dati sensibili o critici, anche in assenza di danni diretti accertati;
- presenta potenziali effetti a catena su altri enti, fornitori o servizi esterni interconnessi.

La valutazione della significatività dell'incidente è effettuata caso per caso, sulla base delle informazioni disponibili, adottando un approccio prudenziale.

3.4 Criteri di classificazione degli incidenti

Al fine di garantire uniformità di valutazione, tracciabilità e coerenza decisionale, gli incidenti informatici sono classificati in base alla tipologia di impatto:

- Riservatezza: accesso non autorizzato a dati o informazioni, perdita o divulgazione indebita di informazioni riservate;
- Integrità: alterazione non autorizzata di dati, configurazioni, applicazioni o sistemi;
- Disponibilità: interruzione totale o parziale, o degrado significativo, dei servizi o dei sistemi informativi;

- Incidenti combinati: eventi che coinvolgono contemporaneamente più dimensioni (ad esempio perdita di dati e indisponibilità dei servizi).

La classificazione non esclude che un incidente possa evolvere nel tempo e ricadere in più categorie.

3.5 Indicatori di gravità dell'incidente

La gravità di un incidente informatico è determinata sulla base di una valutazione complessiva che tiene conto, tra gli altri, dei seguenti indicatori:

- numero e tipologia dei sistemi coinvolti;
- numero di utenti interni o esterni impattati;
- durata dell'indisponibilità o del degrado del servizio;
- tipologia, quantità e criticità dei dati coinvolti;
- impatto sui processi istituzionali e sui servizi erogati;
- potenziali conseguenze legali, economiche o reputazionali;
- capacità di propagazione dell'incidente e difficoltà di contenimento.

Gli indicatori di gravità sono documentati nella fase di analisi dell'incidente e costituiscono la base per le decisioni relative all'escalation e alla notifica.

3.6 Collegamento con la notifica esterna

La classificazione dell'incidente e la valutazione della sua gravità costituiscono il presupposto per:

- determinare l'obbligo di notifica verso l'autorità competente (ACN);
- definire le tempistiche di notifica previste dalla normativa;
- predisporre le informazioni e le evidenze documentali da trasmettere.

In caso di incertezza sulla significatività dell'incidente, è adottato un approccio prudenziale, privilegiando la notifica rispetto all'omissione, nel rispetto dei principi di proporzionalità e responsabilità.

3.7 Esempi di incidenti informatici

A titolo esemplificativo e non esaustivo, rientrano tra gli incidenti informatici:

- compromissione di credenziali con accesso non autorizzato a sistemi dell'Ente;
- infezione da malware o ransomware su sistemi di produzione;
- perdita, esfiltrazione o accesso non autorizzato a dati personali o sensibili;
- attacchi che causano indisponibilità prolungata dei servizi digitali;
- incidenti che coinvolgono fornitori con accesso ai sistemi informativi dell'Ente.

Gli esempi riportati hanno esclusivamente finalità operative e non sostituiscono la valutazione puntuale dell'incidente effettuata caso per caso.

CAPITOLO 4 – GOVERNANCE DELLA GESTIONE DEGLI INCIDENTI INFORMATICI

4.1 Principi generali di governance

La governance della gestione degli incidenti informatici dell'Agenzia Interregionale per il fiume Po (AIPo) è improntata ai principi di unitarietà, coordinamento, responsabilità e tracciabilità.

Tali principi garantiscono che il processo di gestione degli incidenti sia svolto in modo coerente, proporzionato e documentato, indipendentemente dalla natura e dall'origine dell'evento.

L'AIPo mantiene in ogni caso la responsabilità complessiva e il governo del processo di gestione degli incidenti informatici, anche quando alcune attività operative siano affidate a soggetti in house o a fornitori esterni.

Il modello di governance adottato è finalizzato a garantire che ogni incidente informatico sia gestito in modo strutturato, con chiara attribuzione dei ruoli, flussi decisionali definiti e adeguata documentazione delle attività svolte.

4.2 Struttura organizzativa per la gestione degli incidenti

La gestione degli incidenti informatici è assicurata attraverso una struttura organizzativa che coinvolge, secondo le rispettive competenze e responsabilità, gli organi di vertice dell'Ente, Il Responsabile per la Transizione Digitale, Il Dirigente ICT , il Referente per la cybersicurezza, la struttura ICT, gli amministratori di sistema, il Responsabile della protezione dei dati e, ove necessario, i soggetti in house che supportano l'AIPo nella gestione di specifici ambiti dei sistemi informativi.

La struttura opera secondo un modello di escalation progressiva, che consente di modulare il livello di coinvolgimento delle diverse figure in funzione della gravità e della natura dell'incidente.

4.3 Organi di vertice dell'Ente

Gli organi di vertice dell'AIPo esercitano le funzioni di indirizzo, supervisione e responsabilità ultima in materia di sicurezza informatica e gestione degli incidenti, nel rispetto della normativa vigente.

In tale ambito, gli organi di vertice:

- assicurano l'adozione, l'approvazione e l'aggiornamento del presente Manuale;
- sono informati in merito agli incidenti informatici di particolare rilevanza o significatività;
- assumono le decisioni strategiche nei casi in cui l'incidente presenti impatti rilevanti sull'Ente;
- garantiscono il supporto organizzativo e le risorse necessarie per una gestione efficace degli incidenti.
-

4.4 Referente per la cybersicurezza

Il Referente per la cybersicurezza coordina operativamente il processo di gestione degli incidenti informatici ed è il punto di riferimento interno per le attività previste dal presente Manuale.

In particolare, il Referente per la cybersicurezza:

- riceve e coordina la gestione delle segnalazioni di incidente;
- assicura la classificazione e la valutazione della gravità degli eventi;
- coordina le attività di analisi, contenimento, mitigazione e ripristino;
- valuta la necessità di attivare l'escalation interna e le procedure di notifica;
- garantisce la tracciabilità e la documentazione delle attività svolte;
- mantiene il registro degli incidenti informatici dell'Ente.

Il Referente per la cybersicurezza opera in raccordo con la struttura ICT, con gli amministratori di sistema e con i soggetti in house, assicurando il coordinamento complessivo del processo di gestione.

4.5 Struttura ICT e amministratori di sistema

La struttura ICT dell'AIPo è responsabile delle attività tecniche e operative di gestione degli incidenti informatici, in coordinamento con il Referente per la cybersicurezza e nel rispetto delle procedure previste dal presente Manuale.

Gli amministratori di sistema svolgono le attività tecniche specialistiche necessarie alla gestione degli incidenti, incluse le operazioni di analisi, contenimento, mitigazione e ripristino dei sistemi, e sono tenuti a documentare le proprie attività in modo puntuale e tempestivo.

4.6 Ruolo dei soggetti in house nella gestione degli incidenti

L'AIPo si avvale, per la gestione di specifici ambiti dei propri sistemi informativi, di soggetti in house che operano nell'ambito di specifici rapporti convenzionali o contrattuali.

In particolare:

- CSI Piemonte supporta l'AIPo nella gestione di una parte significativa dei sistemi applicativi e dei servizi gestiti in ambiente cloud;
- Lepida fornisce servizi relativi all'infrastruttura di rete e all'ospitalità dei sistemi in ambiente cloud certificato.

Il coinvolgimento di tali soggetti in house avviene nell'ambito delle rispettive competenze tecniche e non comporta il trasferimento della responsabilità complessiva del processo di gestione degli incidenti.

I soggetti in house operano su attivazione dell'Ente e in coordinamento con il Referente per la cybersicurezza e la struttura ICT, secondo le modalità previste dagli accordi in essere e dalle procedure del presente Manuale.

4.7 Responsabile della protezione dei dati

Il Responsabile della protezione dei dati è coinvolto nei casi in cui l'incidente informatico comporti o possa comportare una violazione dei dati personali, ai sensi della normativa vigente in materia di protezione dei dati (GDPR — Reg. UE 2016/679 — e D.Lgs. 196/2003 come modificato).

Il coinvolgimento avviene al fine di valutare gli impatti sulla protezione dei dati, supportare l'individuazione delle misure di mitigazione appropriate e, ove necessario, attivare le procedure di notifica al Garante per la protezione dei dati personali e di comunicazione agli interessati.

4.8 Flussi decisionali ed escalation

La gestione degli incidenti informatici prevede flussi decisionali chiari e livelli di escalation proporzionati alla gravità e all'impatto dell'evento. Il Referente per la cybersicurezza è il punto di raccordo delle informazioni e il coordinatore delle decisioni operative.

Gli incidenti di minore impatto sono gestiti a livello operativo, sotto il coordinamento del Referente per la cybersicurezza. Gli incidenti significativi o ad alto impatto richiedono il coinvolgimento degli organi di vertice e, ove necessario, l'attivazione delle procedure di notifica esterna.

Ogni decisione rilevante è assunta in modo motivato e documentato.

4.9 Coordinamento e responsabilità complessiva

La governance della gestione degli incidenti informatici è esercitata dall'AIPo in modo unitario e coordinato, anche quando le attività operative siano distribuite tra più soggetti interni o esterni.

L'AIPo mantiene in ogni fase il controllo del processo decisionale, della comunicazione istituzionale e della documentazione delle attività

CAPITOLO 5 – PROCESSO DI SEGNALAZIONE INTERNA DEGLI INCIDENTI INFORMATICI

5.1 Il ruolo della segnalazione nella sicurezza dell'Ente

La segnalazione tempestiva di eventi anomali o sospetti costituisce uno degli elementi più importanti del sistema di sicurezza informatica dell'AIPo. La capacità di rilevare e comunicare prontamente un potenziale incidente è determinante per limitarne l'impatto e per garantire una risposta efficace.

Ogni dipendente, collaboratore o soggetto che opera sui sistemi dell'Ente rappresenta quindi un presidio attivo della sicurezza informatica e ha la responsabilità di contribuire al sistema di rilevazione degli incidenti attraverso la segnalazione di qualsiasi anomalia o evento sospetto.

5.2 Chi è tenuto a segnalare

La segnalazione di un potenziale incidente informatico non è riservata al solo personale tecnico o alla struttura ICT. È dovere di tutto il personale dell'AIPo, nonché di qualsiasi soggetto esterno che operi sui sistemi informativi dell'Ente, segnalare tempestivamente qualsiasi anomalia o evento sospetto di cui venga a conoscenza.

Ogni persona che rilevi un comportamento anomalo, un malfunzionamento insolito o una situazione che non trova una spiegazione ordinaria nell'ambito del normale funzionamento dei sistemi informativi dell'Ente è tenuta a procedere immediatamente alla segnalazione.

È sempre preferibile una segnalazione in più rispetto a una in meno, anche quando sussistono dubbi sulla reale gravità dell'evento o sulla sua riconducibilità a un incidente informatico.

5.3 Quando effettuare una segnalazione

Il principio che guida il processo di segnalazione è semplice: ogni situazione che si discosta dal normale funzionamento dei sistemi, dei dispositivi o delle applicazioni deve essere segnalata senza ritardo.

La segnalazione deve avvenire ogni volta che si riscontra un comportamento insolito dei dispositivi o delle applicazioni in uso, difficoltà di accesso a sistemi o risorse normalmente disponibili, comunicazioni sospette ricevute via e-mail, messaggistica o altri canali digitali, accessi o operazioni non riconosciuti, o qualsiasi altra situazione che possa fare ragionevolmente ritenere che la sicurezza dei sistemi informativi possa essere compromessa.

Non è necessario che l'evento abbia già prodotto un danno concreto. Anche situazioni che potrebbero evolvere in un incidente rientrano nell'obbligo di segnalazione.

5.4 Anomalie e situazioni che richiedono segnalazione

Esistono alcune situazioni che, per loro natura, devono essere sempre segnalate senza ritardo. Tra queste rientrano, a titolo esemplificativo: la ricezione di messaggi di posta elettronica con

contenuti sospetti o richieste inusuali; l'apertura accidentale di allegati o link potenzialmente malevoli; la visualizzazione di messaggi di errore inusuali o richieste di riscatto (ransomware); la perdita o il furto di dispositivi aziendali; l'impossibilità di accedere a sistemi o dati normalmente disponibili; qualsiasi modifica non autorizzata a dati, configurazioni o impostazioni di sistema.

In tutti questi casi, il dipendente non deve tentare di risolvere autonomamente il problema, ma limitarsi a segnalare l'anomalia ai soggetti competenti, preservando le evidenze disponibili.

5.5 Segnalazione di errori involontari

Anche gli errori commessi in buona fede devono essere segnalati. L'apertura accidentale di un allegato sospetto, l'invio di informazioni a destinatari errati o qualsiasi altra azione involontaria che possa avere impatti sulla sicurezza dei sistemi dell'Ente devono essere comunicati tempestivamente.

La segnalazione di errori involontari non comporta automaticamente responsabilità disciplinari. Al contrario, la trasparenza e la tempestività della segnalazione sono elementi che l'Ente considera positivamente nell'ambito della gestione degli incidenti.

5.6 Comportamenti da evitare in caso di sospetto incidente

In presenza di un sospetto incidente informatico, il segnalante non deve intraprendere iniziative autonome di natura tecnica volte a risolvere il problema, modificare le configurazioni di sistema, cancellare file o log, o tentare di ripristinare autonomamente la normalità operativa.

Questi comportamenti potrebbero compromettere la possibilità di analizzare correttamente l'evento e di conservare le evidenze necessarie per la gestione dell'incidente e per eventuali adempimenti normativi.

5.7 Responsabilità del segnalante

Il ruolo del segnalante consiste nel comunicare quanto osservato in modo chiaro e tempestivo, fornendo le informazioni disponibili senza interpretazioni tecniche o valutazioni di gravità che non rientrano nelle proprie competenze.

La responsabilità principale del segnalante è quella di non ignorare l'anomalia e di contribuire attivamente alla sicurezza informatica dell'Ente attraverso una segnalazione tempestiva e accurata.

5.8 Modalità di segnalazione interna

La segnalazione di un incidente informatico o di un evento sospetto deve essere effettuata attraverso i canali ufficiali predisposti dall'Ente, con particolare attenzione a garantire tempestività e tracciabilità della comunicazione.

La segnalazione deve essere effettuata non appena l'evento viene rilevato, evitando ritardi non giustificati. Anche in caso di incertezza sulla natura o sulla gravità dell'evento, la segnalazione deve avvenire tempestivamente, senza attendere la raccolta di ulteriori informazioni.

La segnalazione può essere effettuata direttamente dal soggetto che rileva l'evento oppure, in caso di difficoltà, tramite il proprio responsabile diretto.

5.9 Canali di segnalazione

L'Ente individua specifici canali di segnalazione interna, progettati per assicurare accessibilità, continuità operativa e tracciabilità delle comunicazioni. I canali primari includono il sistema di ticketing ICT dell'Ente (helpdesk@agenziapo.it), la posta elettronica del referente per la Cybersicurezza (cybersicurezza@agenziapo.it) e, per le urgenze, il recapito telefonico del Referente per la cybersicurezza reperibile sul sito istituzionale dell'Ente.

Le modalità e i recapiti dei canali di segnalazione sono resi noti al personale e periodicamente aggiornati.

5.10 Contenuto della segnalazione

La segnalazione deve contenere, per quanto possibile, una descrizione chiara e comprensibile dell'evento osservato, con le informazioni disponibili al momento della rilevazione.

In particolare, il segnalante è invitato a indicare: cosa è stato osservato; quando si è verificato l'evento; su quale dispositivo, sistema o applicazione; il nome utente o le credenziali eventualmente coinvolte; le azioni eventualmente già intraprese e qualsiasi altra informazione ritenuta rilevante.

La mancanza di alcune informazioni non preclude la validità della segnalazione. È preferibile una segnalazione incompleta ma tempestiva rispetto a una segnalazione tardiva ma esaustiva.

5.11 Presa in carico della segnalazione

Una volta ricevuta, la segnalazione viene presa in carico dalla struttura competente, che ne verifica la completezza minima e provvede ad avviare le attività di valutazione preliminare dell'evento segnalato.

Il segnalante può essere contattato per chiarimenti o integrazioni, qualora necessario. La presa in carico della segnalazione è documentata e il segnalante riceve, nei limiti del possibile, una conferma dell'avvenuta ricezione.

La presa in carico non implica automaticamente che l'evento segnalato sia classificato come incidente informatico. La valutazione definitiva è effettuata nella fase successiva di analisi.

5.12 Gestione della segnalazione e aggiornamenti

Nel corso della gestione dell'evento, le strutture competenti valutano l'evoluzione della situazione e adottano le misure previste dal presente Manuale.

Il segnalante viene informato, nei limiti del principio di riservatezza e di necessità di conoscere, sull'esito della valutazione della segnalazione e sulle eventuali azioni intraprese.

La gestione della segnalazione può comportare l'attivazione di ulteriori procedure previste dal presente Manuale, incluse quelle relative alla classificazione e alla notifica degli incidenti.

5.13 Tracciabilità e conservazione delle informazioni

Tutte le segnalazioni e le attività connesse alla loro gestione sono oggetto di tracciabilità. Le informazioni raccolte nel corso del processo di segnalazione sono conservate in modo da consentire la ricostruzione dell'iter seguito e la verifica delle azioni intraprese.

La documentazione relativa alle segnalazioni costituisce parte integrante delle evidenze a disposizione dell'Ente ai fini della gestione degli incidenti, del miglioramento continuo e dell'adempimento degli obblighi normativi.

5.14 Valore della segnalazione nel processo di sicurezza

Ogni segnalazione, indipendentemente dall'esito finale, rappresenta un elemento di valore per il sistema di sicurezza informatica dell'AIPo e contribuisce a migliorare la capacità di rilevazione e risposta agli incidenti.

Il processo di segnalazione non deve essere percepito come un adempimento formale, ma come uno strumento di collaborazione attiva alla sicurezza dell'Ente, fondamentale per garantire la continuità operativa e la protezione dei dati e delle infrastrutture digitali dell'AIPo.

CAPITOLO 6 – PROCESSO DI GESTIONE DELL'INCIDENTE INFORMATICO

6.1 Finalità del processo di gestione dell'incidente

Il processo di gestione dell'incidente informatico ha la finalità di garantire una risposta tempestiva, coordinata e proporzionata agli eventi che compromettano o possano compromettere la sicurezza dei sistemi informativi dell'AIPo.

Attraverso l'applicazione delle procedure descritte nel presente capitolo, l'AIPo assicura che ogni incidente sia gestito in modo strutturato, con chiara attribuzione delle responsabilità, adeguata documentazione delle attività e raccordo con le procedure di notifica esterna ove necessario.

Il processo di gestione dell'incidente è strettamente connesso al processo di segnalazione interna ed è attivato a seguito della presa in carico di una segnalazione che presenti le caratteristiche di un incidente informatico.

6.2 Attivazione del processo di gestione

Il processo di gestione dell'incidente informatico è attivato nel momento in cui una segnalazione viene formalmente presa in carico dal Referente per la cybersicurezza e ritenuta idonea ad avviare le procedure previste dal presente Manuale.

L'attivazione del processo non presuppone, in questa fase iniziale, una classificazione definitiva dell'evento. È sufficiente la ragionevole ritenuta esistenza di un evento che possa qualificarsi come incidente informatico.

L'attivazione del processo è sempre documentata, anche nel caso in cui l'evento venga successivamente riclassificato come evento di sicurezza privo di impatto rilevante.

6.3 Presa in carico dell'incidente

A seguito dell'attivazione, l'incidente è formalmente preso in carico dal Referente per la cybersicurezza, che assume il coordinamento operativo del processo di gestione e garantisce il raccordo tra le strutture coinvolte.

Qualora l'incidente informatico riguardi sistemi, applicazioni o infrastrutture la cui gestione operativa è affidata a soggetti in house (CSI Piemonte, Lepida), il Referente per la cybersicurezza provvede ad attivare tempestivamente il coinvolgimento degli stessi.

La presa in carico consiste nell'avvio delle attività di analisi preliminare e nella verifica delle informazioni contenute nella segnalazione, al fine di acquisire una prima comprensione della natura e dell'estensione dell'evento.

6.4 Analisi preliminare dell'incidente

L'analisi preliminare ha lo scopo di acquisire una prima comprensione dell'evento segnalato, al fine di orientare le successive fasi di gestione.

In questa fase vengono esaminate le informazioni fornite dal segnalante, i dati tecnici disponibili, i log di sistema e qualsiasi altra evidenza utile a ricostruire le circostanze dell'evento.

L'analisi preliminare è condotta dalla struttura ICT, sotto il coordinamento del Referente per la cybersicurezza, e si conclude con una prima valutazione della natura e dell'estensione dell'incidente.

Ove necessario, l'analisi preliminare può avvalersi del supporto tecnico dei soggetti in house che gestiscono specifici ambiti dei sistemi interessati dall'incidente, attivati su richiesta del Referente per la cybersicurezza.

6.5 Valutazione iniziale dell'impatto e della gravità

Sulla base degli esiti dell'analisi preliminare, viene effettuata una prima valutazione dell'impatto potenziale e della gravità dell'incidente, con riferimento agli indicatori definiti al paragrafo 3.5 del presente Manuale.

Tale valutazione tiene conto, in particolare, dell'eventuale compromissione della disponibilità, dell'integrità o della riservatezza dei sistemi o dei dati interessati, nonché del potenziale impatto sui servizi istituzionali e sui soggetti coinvolti.

La valutazione dell'impatto e della gravità può essere aggiornata nel corso della gestione dell'incidente, man mano che si acquisiscono nuove informazioni.

6.6 Classificazione provvisoria dell'incidente

All'esito dell'analisi preliminare e della valutazione iniziale, l'incidente è oggetto di una classificazione provvisoria, secondo i criteri definiti al paragrafo 3.4 del presente Manuale.

La classificazione provvisoria consente di orientare le successive fasi di gestione, in particolare quelle relative al contenimento e alla mitigazione dell'incidente, e di valutare la necessità di attivare le procedure di notifica.

La classificazione provvisoria non pregiudica la possibilità di una successiva riclassificazione dell'incidente, qualora emergano nuove informazioni nel corso della gestione.

6.7 Tracciabilità delle attività iniziali

Tutte le attività svolte nelle fasi di attivazione, presa in carico e analisi preliminare dell'incidente sono oggetto di documentazione sistematica, con indicazione delle azioni intraprese, dei soggetti coinvolti e dei tempi di esecuzione.

La tracciabilità delle attività costituisce elemento essenziale sia ai fini della gestione operativa dell'incidente sia ai fini degli adempimenti normativi e della verifica dell'adeguatezza delle misure adottate.

6.8 Finalità delle fasi di contenimento e mitigazione

Le fasi di contenimento e mitigazione dell'incidente informatico sono finalizzate a limitare, nel più breve tempo possibile, la diffusione e l'impatto dell'evento, a preservare le evidenze disponibili e a ripristinare le condizioni di sicurezza dei sistemi e dei servizi interessati.

Tali fasi sono attuate secondo criteri di proporzionalità e gradualità, tenendo conto della natura dell'incidente, dell'impatto delle misure adottate sui servizi in corso di erogazione e delle priorità operative dell'Ente.

6.9 Attività di contenimento dell'incidente

Il contenimento dell'incidente consiste nell'adozione di misure immediate volte a circoscrivere l'evento, impedire la sua propagazione e limitarne l'impatto sui sistemi e sui servizi dell'Ente.

Qualora le attività di contenimento riguardino sistemi o infrastrutture gestite da soggetti in house, l'attuazione avviene su attivazione del Referente per la cybersicurezza, in coordinamento con i referenti tecnici dei soggetti coinvolti.

Le misure di contenimento possono comportare, a titolo esemplificativo, l'isolamento di sistemi o reti, la sospensione temporanea di servizi, la revoca di credenziali di accesso o l'attivazione di misure di protezione aggiuntive.

Ogni intervento di contenimento è documentato e motivato, al fine di garantire la tracciabilità delle decisioni assunte e la possibilità di valutarne l'efficacia nella fase post-incidente.

6.10 Attività di mitigazione dell'incidente

La mitigazione dell'incidente ha lo scopo di ridurre l'impatto residuo dell'evento e di rimuovere, ove possibile, le cause e le vulnerabilità che hanno consentito o favorito il verificarsi dell'incidente.

In questa fase vengono adottate le misure tecniche e organizzative necessarie a eliminare o ridurre le vulnerabilità sfruttate, a ripristinare le configurazioni di sicurezza appropriate e a garantire la protezione dei dati e dei sistemi.

La fase di mitigazione è condotta in modo coordinato con le attività di contenimento e può estendersi nel tempo, in funzione della complessità dell'incidente e delle risorse disponibili.

6.11 Ripristino dei sistemi e dei servizi

Conclusa la fase di contenimento e avviate le misure di mitigazione, l'AIPo procede al ripristino dei sistemi e dei servizi interessati dall'incidente, garantendo che le condizioni di sicurezza siano adeguatamente verificate prima della reimmissione in produzione.

Il ripristino avviene secondo modalità controllate, evitando il ripristino di sistemi o servizi in condizioni che possano esporre l'Ente a ulteriori rischi.

Nel caso di sistemi o servizi la cui gestione operativa è affidata a soggetti in house, le attività di ripristino sono svolte in coordinamento con gli stessi, su attivazione del Referente per la cybersicurezza.

Le attività di ripristino sono coordinate dalla struttura ICT e documentate in modo puntuale.

6.12 Coordinamento con la continuità operativa

Nel caso in cui l'incidente informatico abbia un impatto rilevante sulla continuità operativa dell'Ente, le procedure di gestione dell'incidente sono coordinate con le misure di continuità operativa adottate dall'AIPo.

Il coordinamento tra gestione dell'incidente e continuità operativa consente di assicurare la priorità al mantenimento dei servizi essenziali e di minimizzare l'impatto dell'evento sull'operatività dell'Ente.

6.13 Aggiornamento della valutazione dell'incidente

Nel corso delle fasi di contenimento, mitigazione e ripristino, la valutazione dell'incidente è costantemente aggiornata sulla base delle nuove informazioni acquisite.

L'evoluzione dell'evento può comportare la revisione della classificazione iniziale dell'incidente, l'attivazione di ulteriori misure di gestione o la modifica delle decisioni relative alla notifica esterna.

Ogni aggiornamento rilevante è adeguatamente documentato.

6.14 Conclusione della gestione operativa

La gestione operativa dell'incidente può dirsi conclusa quando i sistemi e i servizi interessati sono stati ripristinati in condizioni di sicurezza, le cause dell'incidente sono state adeguatamente identificate e le misure di mitigazione sono state attuate.

La conclusione della gestione operativa non esclude lo svolgimento di ulteriori attività di analisi, valutazione e miglioramento previste dalla fase post-incidente, disciplinata al Capitolo 9 del presente Manuale.

CAPITOLO 7 – NOTIFICA E COMUNICAZIONI VERSO L'ESTERNO

7.1 Finalità della notifica degli incidenti informatici

La notifica degli incidenti informatici verso soggetti esterni costituisce un adempimento rilevante ai fini del rispetto della normativa vigente e contribuisce al rafforzamento del sistema nazionale di cybersicurezza.

Attraverso la notifica, l'Agenzia Interregionale per il fiume Po (AIPo) contribuisce al sistema di sicurezza cibernetica nazionale, fornendo informazioni utili all'Agenzia per la Cybersicurezza Nazionale (ACN) per l'analisi delle minacce e il coordinamento delle risposte.

La notifica non ha natura sanzionatoria, ma preventiva e collaborativa, ed è finalizzata a rafforzare la resilienza complessiva del sistema informatico nazionale.

7.2 Ambito di applicazione delle notifiche

Le disposizioni del presente capitolo disciplinano le modalità con cui l'AIPo effettua le comunicazioni e le notifiche verso soggetti esterni in relazione agli incidenti informatici, con particolare riferimento alle notifiche verso l'Autorità competente NIS (ACN).

Rientrano nell'ambito di applicazione del presente capitolo gli incidenti informatici che, in base alla valutazione effettuata ai sensi del Capitolo 3, presentano caratteristiche tali da richiedere la notifica verso l'esterno.

7.3 Presupposti per l'attivazione della notifica

La decisione di procedere alla notifica di un incidente informatico verso l'esterno è assunta a seguito della valutazione della gravità e dell'impatto dell'evento, effettuata dal Referente per la cybersicurezza in coordinamento con le strutture competenti.

La notifica è attivata quando l'incidente:

- ha causato o può causare un impatto rilevante sulla continuità dei servizi dell'Ente;
- ha interessato o può interessare dati, sistemi o infrastrutture critiche;
- presenta caratteristiche tali da richiedere il coinvolgimento o l'informazione delle autorità competenti.

In caso di incertezza circa la sussistenza dei presupposti per la notifica, l'AIPo adotta un approccio prudenziale, privilegiando la notifica rispetto all'omissione.

7.4 Soggetto responsabile della notifica

La responsabilità della notifica degli incidenti informatici verso l'esterno è in capo all'Agenzia Interregionale per il fiume Po (AIPo), che ne risponde nei confronti delle autorità competenti.

La predisposizione e l'invio delle notifiche sono attivate e coordinate dal Referente per la cybersicurezza, che opera in raccordo con gli organi di vertice dell'Ente e con le strutture competenti.

Il coinvolgimento di soggetti in house o di altri fornitori non comporta in alcun caso il trasferimento della responsabilità della notifica, che rimane in capo all'AIPo.

7.5 Coordinamento interno prima della notifica

Prima dell'invio della notifica verso l'esterno, è assicurato un adeguato coordinamento interno, finalizzato a garantire la completezza, la coerenza e l'accuratezza delle informazioni trasmesse.

Il coordinamento interno consente di:

- consolidare le informazioni tecniche e organizzative disponibili;
- valutare l'evoluzione dell'incidente e i possibili impatti;
- garantire l'allineamento tra le strutture coinvolte;
- evitare comunicazioni frammentarie o non coerenti.

Il coordinamento interno non deve tuttavia comportare ritardi ingiustificati nell'invio della notifica, nel rispetto delle tempistiche previste dalla normativa vigente (D.Lgs. 138/2024, art. 24: preallarme entro 24 ore, notifica entro 72 ore).

7.6 Tracciabilità della decisione di notifica

La decisione di procedere o meno alla notifica di un incidente informatico è sempre oggetto di documentazione.

Sono tracciate:

- le valutazioni effettuate;
- i soggetti coinvolti nel processo decisionale;
- le motivazioni alla base della decisione assunta;
- i tempi e le modalità della comunicazione verso l'esterno.
-

7.7 Tempistiche della notifica

La notifica degli incidenti informatici verso l'esterno è effettuata nel rispetto delle tempistiche previste dalla normativa vigente, con particolare riferimento alle disposizioni del D.Lgs. 138/2024 (recepimento NIS2): preallarme entro 24 ore dalla presa di consapevolezza, notifica iniziale entro 72 ore, relazione finale entro un mese.

Le tempistiche decorrono dal momento in cui l'AIPo acquisisce una ragionevole consapevolezza del verificarsi di un incidente significativo, indipendentemente dalla completezza delle informazioni disponibili.

Nel corso della gestione dell'incidente, l'AIPo assicura che le comunicazioni verso l'esterno siano costantemente aggiornate, in funzione dell'evoluzione dell'evento.

7.8 Contenuto della notifica iniziale

La notifica iniziale dell'incidente informatico ha lo scopo di fornire alle autorità competenti una prima informazione sull'evento, in modo da consentire l'attivazione tempestiva delle misure di supporto e coordinamento.

La notifica contiene, per quanto disponibile al momento dell'invio, una descrizione dell'incidente, delle sue caratteristiche principali, dei sistemi e dei servizi interessati e delle misure già adottate.

La mancanza di alcune informazioni non preclude l'invio della notifica iniziale, purché l'AIPo si impegni a fornire gli aggiornamenti successivi man mano che le informazioni si rendano disponibili.

7.9 Aggiornamenti successivi alla notifica

A seguito della notifica iniziale, l'AIPo fornisce aggiornamenti periodici alle autorità competenti, in relazione all'evoluzione dell'incidente e alle misure adottate.

Gli aggiornamenti successivi consentono di:

- integrare o correggere le informazioni inizialmente trasmesse;
- comunicare l'esito delle attività di contenimento e mitigazione;
- rappresentare lo stato di ripristino dei sistemi e dei servizi;
- segnalare eventuali ulteriori impatti emersi nel corso della gestione.

Gli aggiornamenti sono trasmessi in modo coerente e coordinato, evitando comunicazioni ridondanti o non allineate.

7.10 Comunicazioni di chiusura dell'incidente

Al termine della gestione dell'incidente informatico, l'AIPo provvede, ove previsto, a trasmettere una comunicazione di chiusura alle autorità competenti.

La comunicazione di chiusura fornisce un quadro complessivo dell'incidente, delle cause individuate, delle misure adottate e degli esiti delle attività di ripristino e miglioramento.

7.11 Qualità e coerenza delle informazioni trasmesse

Le informazioni trasmesse nell'ambito delle notifiche e delle comunicazioni verso l'esterno devono essere accurate, complete e coerenti con le evidenze disponibili.

L'AIPo assicura che le comunicazioni siano redatte in modo chiaro e comprensibile, evitando formulazioni ambigue o suscettibili di generare fraintendimenti.

7.12 Tracciabilità delle notifiche e delle comunicazioni

Tutte le notifiche e le comunicazioni verso l'esterno sono oggetto di tracciabilità e conservazione nell'ambito del registro degli incidenti informatici dell'Ente.

Sono conservate le informazioni relative ai contenuti trasmessi, ai tempi di invio, ai destinatari e agli eventuali riscontri ricevuti.

7.13 Coordinamento con soggetti in house e fornitori

Qualora l'incidente informatico riguardi sistemi o infrastrutture la cui gestione operativa è affidata a soggetti in house, l'AIPo assicura il necessario coordinamento informativo con gli

stessi, al fine di garantire la completezza delle informazioni da trasmettere alle autorità competenti.

Il coordinamento informativo non comporta in alcun caso il trasferimento della responsabilità della comunicazione verso l'esterno, che rimane in capo all'AIPo.

CAPITOLO 8 – COMUNICAZIONI INTERNE ED ESTERNE

8.1 Finalità delle comunicazioni in caso di incidente informatico

Le comunicazioni interne ed esterne connesse alla gestione di un incidente informatico hanno la finalità di assicurare un flusso informativo ordinato, proporzionato e coerente tra i soggetti coinvolti nella gestione dell'evento.

Una gestione ordinata delle comunicazioni consente all'Agenzia Interregionale per il fiume Po (AIPo) di tutelare la propria immagine istituzionale, di garantire la riservatezza delle informazioni sensibili e di assicurare il rispetto degli obblighi normativi in materia di comunicazione.

8.2 Principi generali delle comunicazioni

Le comunicazioni connesse a incidenti informatici sono improntate ai principi di necessità, proporzionalità, riservatezza e coerenza.

Le informazioni sono condivise esclusivamente con i soggetti che, in relazione al ruolo ricoperto, hanno necessità di conoscerle ai fini della gestione dell'incidente o dell'adempimento degli obblighi normativi.

8.3 Comunicazioni interne

Nel corso della gestione di un incidente informatico, l'AIPo assicura adeguate comunicazioni interne al fine di garantire il coordinamento tra le strutture coinvolte e il necessario flusso informativo verso gli organi di vertice.

Le comunicazioni interne sono effettuate secondo livelli di dettaglio differenziati, in funzione del ruolo dei destinatari e della natura delle informazioni da trasmettere.

Le comunicazioni interne sono gestite in modo da evitare la diffusione indiscriminata di informazioni e il rischio di interferenze con le attività di gestione dell'incidente.

8.4 Comunicazioni verso il personale dell'Ente

Qualora l'incidente informatico renda necessario informare il personale dell'Ente, le comunicazioni sono predisposte dal Referente per la cybersicurezza, in coordinamento con gli organi di vertice.

Le comunicazioni verso il personale possono riguardare, ad esempio, limitazioni temporanee nell'uso di determinati sistemi o applicazioni, istruzioni operative specifiche da seguire nel corso della gestione dell'incidente o informazioni generali sull'evento.

8.5 Comunicazioni verso soggetti esterni diversi dalle autorità competenti

Le comunicazioni verso soggetti esterni diversi dalle autorità competenti, quali fornitori, partner o altri enti, sono effettuate dall'AIPo sulla base di una valutazione della necessità e dell'opportunità della comunicazione.

Tali comunicazioni sono coordinate dall'AIPo e avvengono nel rispetto dei principi di riservatezza e minimizzazione delle informazioni condivise.

8.6 Comunicazioni verso utenti, cittadini o altri destinatari esterni

Nel caso in cui un incidente informatico possa avere impatti sui servizi erogati all'esterno, l'AIPo valuta l'opportunità di informare gli utenti, i cittadini o altri destinatari interessati, nel rispetto dei principi di trasparenza e proporzionalità.

Tali comunicazioni sono predisposte in forma istituzionale, con contenuti chiari e comprensibili, limitati alle informazioni necessarie per consentire ai destinatari di adottare le misure di cautela del caso.

8.7 Autorizzazione e responsabilità delle comunicazioni

Le comunicazioni connesse a incidenti informatici sono effettuate esclusivamente da soggetti autorizzati dall'AIPo, nell'ambito delle rispettive competenze istituzionali.

In particolare, le comunicazioni istituzionali verso l'esterno sono predisposte con il coordinamento del Referente per la cybersicurezza e approvate dagli organi di vertice.

Il personale dell'Ente non è autorizzato a rilasciare dichiarazioni o informazioni verso l'esterno in merito a incidenti informatici, salvo specifica autorizzazione.

8.8 Coordinamento con la gestione dell'incidente

Le comunicazioni interne ed esterne sono costantemente coordinate con lo stato di avanzamento della gestione dell'incidente, al fine di garantire la coerenza e l'accuratezza delle informazioni trasmesse.

Qualora l'evoluzione dell'incidente renda necessario aggiornare le comunicazioni già effettuate, l'AIPo provvede tempestivamente a trasmettere le informazioni aggiornate ai destinatari interessati.

8.9 Tracciabilità delle comunicazioni

Le comunicazioni rilevanti effettuate nell'ambito della gestione di un incidente informatico sono oggetto di tracciabilità e conservazione.

La documentazione delle comunicazioni costituisce parte integrante delle evidenze a disposizione dell'AIPo e contribuisce alla ricostruzione complessiva della gestione dell'incidente.

CAPITOLO 9 – GESTIONE POST-INCIDENTE E MIGLIORAMENTO CONTINUO

9.1 Finalità della fase post-incidente

La fase di gestione post-incidente ha la finalità di analizzare in modo strutturato gli eventi verificatisi, valutare l'efficacia delle misure adottate e individuare le azioni di miglioramento necessarie a ridurre il rischio di ricorrenza dell'incidente.

Tale fase consente di trasformare l'esperienza maturata nella gestione dell'incidente in un'opportunità di apprendimento e miglioramento del sistema di sicurezza informatica dell'Ente.

9.2 Chiusura formale dell'incidente

Al termine delle attività di gestione operativa, l'incidente informatico è oggetto di chiusura formale.

La chiusura formale avviene a seguito della verifica del ripristino dei sistemi e dei servizi in condizioni di sicurezza, dell'adozione delle principali misure di mitigazione e della conclusione delle attività di notifica verso l'esterno.

La chiusura formale non preclude l'avvio di ulteriori attività di analisi o approfondimento, qualora ritenuto necessario.

9.3 Analisi dell'incidente e valutazione delle cause

Successivamente alla chiusura formale, l'AIPo procede all'analisi dell'incidente, con l'obiettivo di individuare le cause originarie dell'evento, i fattori che ne hanno favorito il verificarsi e le eventuali carenze nelle misure di sicurezza adottate.

L'analisi tiene conto degli elementi tecnici, organizzativi e procedurali emersi nel corso della gestione dell'incidente, incluse le informazioni fornite dai soggetti in house e dai fornitori eventualmente coinvolti.

L'esito dell'analisi è documentato in modo proporzionato alla rilevanza dell'incidente.

9.4 Valutazione dell'efficacia delle misure adottate

Nel corso della fase post-incidente, l'AIPo valuta l'efficacia delle misure di gestione adottate, con particolare riferimento alla tempestività della risposta, all'adeguatezza delle misure di contenimento e mitigazione e alla qualità della documentazione prodotta.

La valutazione consente di individuare eventuali criticità nei processi, nei flussi informativi o nell'organizzazione delle attività di gestione degli incidenti, al fine di adottare le opportune azioni correttive.

9.5 Individuazione e attuazione delle azioni correttive

Qualora dall'analisi dell'incidente emergano carenze o margini di miglioramento, l'AIPo individua le azioni correttive da adottare e le pianifica in modo proporzionato alla rilevanza dell'incidente e alle risorse disponibili.

Le azioni correttive possono riguardare, a titolo esemplificativo, l'aggiornamento delle configurazioni di sicurezza, il rafforzamento delle procedure operative, la revisione dei controlli di accesso, la formazione del personale o l'aggiornamento della documentazione interna.

L'attuazione delle azioni correttive è pianificata e monitorata, in funzione della rilevanza dell'incidente e dell'urgenza delle misure da adottare.

9.6 Aggiornamento delle misure e dei documenti interni

Gli esiti della gestione post-incidente possono comportare l'aggiornamento delle misure di sicurezza informatica adottate dall'Ente, nonché la revisione dei documenti interni di riferimento, incluso il presente Manuale.

L'aggiornamento dei documenti consente di mantenere allineate le procedure operative all'evoluzione del contesto tecnologico, normativo e organizzativo.

9.7 Formazione e sensibilizzazione

La fase post-incidente può evidenziare la necessità di interventi di formazione o sensibilizzazione del personale.

In tali casi, l'AIPo promuove iniziative volte a rafforzare la consapevolezza in materia di sicurezza informatica e a migliorare la capacità di rilevazione e gestione degli incidenti.

9.8 Miglioramento continuo

La gestione post-incidente si inserisce in un processo di miglioramento continuo del sistema di sicurezza informatica dell'AIPo. Ogni incidente, indipendentemente dalla sua gravità, rappresenta un'opportunità per rafforzare le misure di protezione e la resilienza dell'Ente.

Le informazioni e le evidenze raccolte nel corso della gestione degli incidenti contribuiscono a orientare le scelte organizzative e tecnologiche dell'AIPo in materia di cybersicurezza, in coerenza con i principi di gestione del rischio ICT adottati dall'Ente.

CAPITOLO 10 – CONSERVAZIONE DELLE EVIDENZE E DOCUMENTAZIONE

10.1 Finalità della conservazione delle evidenze

La conservazione delle evidenze relative agli incidenti informatici è finalizzata a garantire la tracciabilità delle attività svolte, la verifica dell'adeguatezza delle misure adottate e l'adempimento degli obblighi normativi in materia di documentazione.

La corretta conservazione della documentazione costituisce elemento essenziale ai fini della responsabilità organizzativa dell'Ente, del miglioramento continuo del sistema di sicurezza informatica e della collaborazione con le autorità competenti in caso di controlli o verifiche.

10.2 Ambito della documentazione oggetto di conservazione

Sono oggetto di conservazione tutte le informazioni e le evidenze prodotte o acquisite nel corso delle fasi di segnalazione, analisi, contenimento, mitigazione, ripristino e notifica dell'incidente informatico.

Rientrano in tale ambito, a titolo esemplificativo, le segnalazioni iniziali, le registrazioni delle attività svolte, le valutazioni di gravità, le decisioni adottate, le comunicazioni interne ed esterne, le notifiche alle autorità competenti e la documentazione relativa alle azioni correttive.

La conservazione delle evidenze è proporzionata alla rilevanza e alla gravità dell'incidente.

10.3 Responsabilità nella gestione della documentazione

La responsabilità della corretta conservazione della documentazione relativa agli incidenti informatici è in capo all'AIPo, che la esercita attraverso il Referente per la cybersicurezza e le strutture competenti.

Il Referente per la cybersicurezza assicura il coordinamento delle attività di raccolta, organizzazione e conservazione della documentazione, garantendo l'integrità e la disponibilità delle evidenze nel tempo.

Il coinvolgimento di soggetti in house o di fornitori esterni nella gestione operativa dell'incidente non comporta il trasferimento della responsabilità della conservazione della documentazione.

10.4 Modalità di conservazione delle evidenze

Le evidenze e la documentazione relative agli incidenti informatici sono conservate in modalità tali da garantirne l'integrità, la riservatezza e la disponibilità nel tempo.

La documentazione è conservata in ambienti e sistemi idonei, con adeguate misure di sicurezza e controlli di accesso, in modo da impedire modifiche non autorizzate o perdite accidentali.

Le modalità di conservazione sono coerenti con le politiche interne dell'Ente in materia di gestione documentale e protezione dei dati.

10.5 Tracciabilità e integrità delle informazioni

La documentazione relativa agli incidenti informatici deve consentire la ricostruzione cronologica delle attività svolte e delle decisioni adottate nel corso della gestione dell'evento.

A tal fine, l'AIPo assicura che le evidenze siano associate a informazioni minime quali la data, il soggetto che ha effettuato l'operazione e il contenuto dell'attività svolta.

Particolare attenzione è riservata alla conservazione delle evidenze tecniche, che devono essere gestite in modo da preservarne l'integrità e l'utilizzabilità ai fini di analisi forensi o verifiche ispettive.

10.6 Tempi di conservazione

Le evidenze e la documentazione relative agli incidenti informatici sono conservate per un periodo di tempo adeguato a soddisfare le esigenze operative, normative e di controllo dell'Ente. In conformità al D.Lgs. 138/2024 e alle indicazioni ACN, il periodo minimo di conservazione è di cinque anni.

I tempi di conservazione tengono conto della rilevanza dell'incidente, della necessità di garantire la disponibilità delle evidenze in caso di controlli o verifiche e degli obblighi normativi applicabili.

Decorso il periodo di conservazione, la documentazione è gestita secondo le procedure interne previste per l'archiviazione e la dismissione dei documenti.

10.7 Utilizzo delle evidenze ai fini di analisi e miglioramento

Le evidenze conservate non sono utilizzate esclusivamente a fini di controllo, ma costituiscono una risorsa per l'analisi degli incidenti e per il miglioramento continuo del sistema di sicurezza informatica dell'Ente.

Le informazioni raccolte possono essere utilizzate per individuare trend, criticità ricorrenti e aree di miglioramento, contribuendo a orientare le scelte organizzative e tecnologiche dell'AIPo in materia di cybersicurezza.

10.8 Disponibilità delle evidenze in caso di verifiche

In caso di controlli, verifiche o ispezioni da parte delle autorità competenti, l'AIPo assicura la disponibilità tempestiva della documentazione relativa agli incidenti informatici.

La disponibilità delle evidenze consente di dimostrare la conformità delle procedure adottate, la correttezza delle decisioni assunte e l'adeguatezza delle misure di gestione degli incidenti implementate dall'Ente.

CAPITOLO 11 – REVISIONE, AGGIORNAMENTO E DIFFUSIONE DEL MANUALE

11.1 Finalità del capitolo

Il presente capitolo disciplina le modalità di revisione, aggiornamento e diffusione del Manuale di segnalazione e gestione degli incidenti informatici, al fine di garantirne la continuità, l'efficacia e l'allineamento al contesto normativo e organizzativo dell'Ente.

La gestione strutturata del ciclo di vita del Manuale assicura che le procedure in esso contenute restino coerenti con l'evoluzione del quadro normativo, delle tecnologie utilizzate e dell'organizzazione dell'AIPo.

11.2 Revisione periodica del Manuale

Il Manuale è soggetto a revisione periodica, con cadenza almeno annuale, ovvero ogni qualvolta si verifichino eventi o circostanze che ne rendano necessario l'aggiornamento.

La revisione periodica è finalizzata a verificare l'efficacia e l'attualità delle procedure descritte, tenendo conto delle novità normative, dei risultati delle attività di gestione degli incidenti e dell'evoluzione delle best practice in materia di cybersicurezza.

11.3 Eventi che comportano l'aggiornamento del Manuale

Fermo restando l'obbligo di revisione periodica, il Manuale è aggiornato in presenza di eventi rilevanti quali, a titolo esemplificativo: modifiche normative significative in materia di cybersicurezza o protezione dei dati; evoluzioni organizzative o tecnologiche rilevanti dell'Ente; gestione di incidenti informatici significativi che evidenzino carenze nelle procedure esistenti; indicazioni o raccomandazioni delle autorità competenti.

L'aggiornamento del Manuale consente di recepire tempestivamente tali cambiamenti, garantendo la coerenza delle procedure operative con il contesto di riferimento.

11.4 Responsabilità della revisione e dell'aggiornamento

La responsabilità del coordinamento delle attività di revisione e aggiornamento del Manuale è attribuita al Referente per la cybersicurezza, in raccordo con il Dirigente ICT (RTD) e le strutture competenti dell'Ente.

Le proposte di aggiornamento sono sottoposte agli organi competenti dell'AIPo per le valutazioni e le approvazioni necessarie.

11.5 Approvazione delle modifiche

Le modifiche al Manuale sono formalmente approvate dagli organi competenti dell'AIPo e acquistano efficacia a decorrere dalla data di pubblicazione, salvo diversa indicazione riportata negli atti.

Le versioni aggiornate del Manuale sostituiscono integralmente le versioni precedenti.

11.6 Diffusione del Manuale

Il Manuale, nella sua versione vigente, è reso disponibile al personale dell'AIPo attraverso le modalità organizzative dell'Ente, inclusa la pubblicazione nell'intranet aziendale e la comunicazione via e-mail a tutti i dipendenti.

L'AIPo assicura che il personale sia adeguatamente informato in merito all'esistenza del Manuale e alle procedure in esso contenute, anche attraverso iniziative di formazione e sensibilizzazione.

11.7 Conservazione delle versioni del Manuale

Le versioni del Manuale, comprese quelle superate, sono conservate al fine di garantire la tracciabilità delle modifiche apportate nel tempo e la possibilità di ricostruire l'evoluzione delle procedure adottate dall'Ente.

La conservazione delle versioni del Manuale avviene in coerenza con le politiche di gestione documentale adottate dall'AIPo.

11.8 Entrata in vigore

Il presente Manuale entra in vigore a decorrere dalla data di approvazione da parte degli organi competenti dell'AIPo, che sarà indicata nell'atto formale di adozione.

A decorrere dalla medesima data, il Manuale costituisce riferimento vincolante per le strutture e il personale dell'AIPo in materia di segnalazione e gestione degli incidenti informatici.