PIANO DI SICUREZZA INFORMATICA
E GESTIONE DEL RISCHIO ICT

Versione:	1.0
Anno:	2026
Approvazione	Comitato di Indirizzo – deliberazione n. 17 del 12 maggio 2026

Sommario

1. Definizioni

Ai fini del presente documento si intende per:

- **Asset ICT:** Qualsiasi componente hardware, software, dato o servizio che abbia valore per l'organizzazione
- **Autenticazione a due fattori (2FA/MFA):** Metodo di autenticazione che richiede due o più fattori di verifica indipendenti
- **Backup:** Copia di sicurezza dei dati finalizzata al ripristino in caso di perdita o corruzione
- **Data breach:** Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali
- **Disaster Recovery:** Insieme di policy e procedure finalizzate al ripristino dei sistemi ICT a seguito di eventi catastrofici
- **Incidente di sicurezza:** Qualsiasi evento che comprometta o minacci di compromettere la riservatezza, integrità o disponibilità dei sistemi informativi
- **Malware:** Software dannoso progettato per danneggiare, interrompere o ottenere accesso non autorizzato a sistemi informatici
- **Phishing:** Tecnica di social engineering finalizzata a sottrarre credenziali o informazioni sensibili mediante comunicazioni fraudolente
- **Ransomware:** Tipo di malware che cripta i dati della vittima richiedendo un riscatto per il ripristino
- **Rischio informatico:** Potenziale evento negativo che può causare danni ai sistemi informativi, valutato in termini di probabilità di accadimento e impatto
- **Sistema informativo:** Insieme organizzato di risorse (hardware, software, dati, procedure, persone) finalizzato alla raccolta, elaborazione, archiviazione e trasmissione delle informazioni
- **Vulnerability:** Debolezza o lacuna in un sistema che può essere sfruttata da una minaccia per comprometterne la sicurezza

2. Premessa e finalità

Il presente documento definisce i principi e l'assetto di governance della sicurezza informatica e della gestione del rischio ICT dell'Agenzia Interregionale per il fiume Po (AIPo), in coerenza con il quadro normativo vigente in materia di cybersicurezza, protezione dei dati personali e amministrazione digitale, nonché con l'evoluzione del contesto tecnologico e organizzativo in cui l'Ente opera.

L'adozione del presente atto si inserisce nel processo di rafforzamento delle misure di sicurezza e resilienza dei sistemi informativi delle pubbliche amministrazioni, anche alla luce della disciplina europea e nazionale in materia di sicurezza delle reti e dei sistemi informativi (Direttiva NIS2 - Direttiva UE 2022/2555, D.Lgs. 138/2024) e delle correlate disposizioni di recepimento, che impongono alle amministrazioni un assetto organizzativo adeguato e proporzionato ai rischi cui sono esposte.

La sicurezza informatica costituisce presupposto essenziale per garantire il buon andamento e l'imparzialità dell'azione amministrativa (art. 97 Cost.), la continuità e l'affidabilità dei servizi istituzionali, la tutela dei dati e delle informazioni trattate (art. 5 GDPR - Reg. UE 2016/679), nonché la protezione dell'integrità e della disponibilità dei sistemi digitali dell'Agenzia.

Il presente documento persegue le seguenti finalità:

- Delineare un quadro unitario di riferimento per la governance della sicurezza ICT
- Chiarire l'assetto delle responsabilità organizzative attraverso la definizione di ruoli e funzioni specifiche
- Definire l'approccio metodologico dell'Ente alla gestione del rischio informatico secondo standard riconosciuti
- Assicurare l'adozione di misure tecniche e organizzative adeguate e proporzionate rispetto ai rischi individuati
- Garantire coerenza sistematica tra i diversi atti e procedure interne in materia di sicurezza digitale

Il documento ha natura di atto di indirizzo e coordinamento organizzativo e non costituisce policy tecnica di dettaglio né regolamento disciplinare. Esso non introduce strumenti di controllo dell'attività lavorativa, né incide sui regimi di responsabilità previsti dalla normativa vigente e dalla disciplina contrattuale applicabile.

3. Quadro normativo di riferimento

Il presente documento si colloca nel seguente quadro normativo:

- Regolamento UE 2016/679 (GDPR) - Protezione dei dati personali, artt. 5, 24, 32
- Direttiva UE 2022/2555 (NIS2) e D.Lgs. 138/2024 - Sicurezza delle reti e dei sistemi informativi
- D.Lgs. 82/2005 (CAD) - Codice dell'Amministrazione Digitale, artt. 51, 71
- D.L. 82/2021 convertito in L. 109/2021 - Istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN)
- L. 90/2024 - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici DPCM 14 novembre 2013 e successive modifiche - Misure minime di sicurezza ICT per le pubbliche amministrazioni
- DPCM 14 novembre 2013 e successive modifiche - Misure minime di sicurezza ICT per le pubbliche amministrazioni
- Circolare AgID n. 1/2017 - Misure minime di sicurezza ICT per le pubbliche amministrazioni
- Linee guida e standard tecnici: ISO/IEC 27001:2022, NIST Cybersecurity Framework, Framework Nazionale per la Cybersecurity ACN

4. Ambito di applicazione

Il presente documento si applica all'insieme dei sistemi informativi, delle infrastrutture digitali, dei servizi ICT e dei dati trattati dall'Agenzia Interregionale per il fiume Po nell'esercizio delle proprie funzioni istituzionali, indipendentemente dalla loro collocazione fisica, dalle modalità di gestione o dalla tecnologia utilizzata.

Rientrano nell'ambito di applicazione:

- Sistemi e servizi digitali gestiti dall'Ente tramite infrastrutture interne on-premise
- Soluzioni in cloud pubblico, privato o ibrido (SaaS, PaaS, IaaS)
- Piattaforme esterne o servizi affidati a soggetti terzi per lo svolgimento di attività istituzionali
- Workstation, dispositivi mobili, endpoint utilizzati dal personale
- Reti dati, infrastrutture di telecomunicazione, apparati di rete
- Banche dati, archivi documentali, sistemi di archiviazione e backup

Le disposizioni del presente documento si estendono, per quanto di competenza, anche ai rapporti con fornitori, partner tecnologici e soggetti in house che concorrono alla progettazione, gestione, manutenzione o erogazione di servizi ICT per conto dell'Ente, nel rispetto delle responsabilità e delle obbligazioni definite nei relativi atti contrattuali o convenzionali.

Resta fermo che le misure di sicurezza applicabili ai singoli sistemi o servizi possono essere ulteriormente specificate in atti, regolamenti o procedure interne di dettaglio (es. Policy di Backup, Policy di Gestione degli Accessi, Procedure Operative Standard), adottati in coerenza con il presente documento.

5. Principi generali di sicurezza informatica

La governance della sicurezza informatica dell'Agenzia si fonda sui seguenti principi generali:

5.1 Triade CIA - Riservatezza, Integrità, Disponibilità

L'Agenzia assicura la tutela della riservatezza (Confidentiality), dell'integrità (Integrity) e della disponibilità (Availability) delle informazioni e dei sistemi informativi, intese quali condizioni essenziali per la regolare erogazione dei servizi istituzionali e per la protezione dei dati trattati secondo quanto previsto dall'art. 32 GDPR.

5.2 Adeguatezza e proporzionalità

L'adozione delle misure di sicurezza avviene secondo il principio di adeguatezza e proporzionalità, in modo da garantire un livello di protezione coerente con:

- La natura e la criticità delle attività svolte
- La tipologia e la sensibilità dei dati trattati
- Il livello di rischio identificato attraverso analisi strutturate
- Le risorse organizzative, tecniche ed economiche disponibili

5.3 Prevenzione e gestione del rischio (Risk-based approach)

L'azione dell'Agenzia è improntata a un approccio risk-based attraverso l'identificazione, valutazione e trattamento dei rischi informatici, integrando la sicurezza nei processi decisionali e organizzativi secondo metodologie strutturate (ISO 31000, ISO/IEC 27005).

5.4 Responsabilità diffusa e coordinata

La sicurezza informatica è concepita quale responsabilità condivisa tra tutti i livelli organizzativi, nel rispetto delle competenze attribuite. Ogni soggetto che opera sui sistemi dell'Ente è tenuto a contribuire al mantenimento della sicurezza secondo il proprio ruolo e le proprie funzioni.

5.5 Miglioramento continuo (Continuous improvement)

La sicurezza informatica si sviluppa secondo una logica di miglioramento continuo (ciclo Plan-Do-Check-Act), in considerazione della costante evoluzione delle minacce, delle tecnologie, delle normative e del contesto organizzativo di riferimento.

5.6 Approccio difesa in profondità- (Defense in depth)

L'Agenzia adotta un approccio a difesa in profondità, implementando controlli di sicurezza su molteplici livelli (fisico, di rete, di sistema, applicativo, dei dati) per garantire che il fallimento di una singola misura non comprometta l'intera sicurezza del sistema.

6. Modello di governance della sicurezza ICT

La sicurezza informatica dell'Agenzia è governata mediante un assetto organizzativo improntato ai principi di responsabilizzazione, coordinamento e integrazione tra i diversi livelli decisionali e operativi, al fine di garantire un approccio unitario, sistematico e coerente alla gestione del rischio ICT.

Il modello di governance si fonda sulla formale individuazione delle funzioni e delle responsabilità in materia di sicurezza informatica, definite mediante specifici provvedimenti organizzativi. Tale formalizzazione assicura:

- La certezza nell'attribuzione delle competenze
- La tracciabilità delle decisioni assunte
- La piena riconducibilità delle scelte organizzative ai soggetti titolari delle funzioni
- La conformità ai principi di responsabilità amministrativa previsti dalla normativa vigente

6.1 Struttura organizzativa e ruoli

La governance della sicurezza ICT si articola attraverso i seguenti ruoli e responsabilità:

Ruolo	Responsabilità principali

Organo di vertice	• Definizione degli indirizzi strategici in materia di sicurezza informatica • Approvazione dei documenti di governance • Vigilanza sull'adeguatezza complessiva dell'assetto organizzativo
Direttore / Dirigente competente ICT / RTD	• Attuazione degli indirizzi generali definiti dal Organo • Coordinamento tra le strutture coinvolte nella gestione ICT • Emanazione di direttive e policy operative in materia di sicurezza • Vigilanza sul rispetto delle policy interne • Allocazione delle risorse necessarie per la cybersecurity
Referente per la Sicurezza ICT	• Coordinamento tecnico-organizzativo delle attività di sicurezza • Predisposizione di policy, procedure e linee guida operative • Monitoraggio dell'attuazione delle misure di sicurezza • Gestione delle relazioni con ACN e altre autorità competenti • Supervisione della gestione degli incidenti di sicurezza • Promozione della cultura della sicurezza e formazione
Ufficio Sistemi Informativi / ICT	• Gestione operativa delle infrastrutture e dei servizi ICT • Implementazione delle misure tecniche di sicurezza • Gestione degli accessi logici e delle identità digitali • Monitoraggio continuo dei sistemi e rilevazione anomalie • Gestione backup, disaster recovery e business continuity • Manutenzione ordinaria e straordinaria dei sistemi
Data Protection Officer (DPO)	• Vigilanza sul rispetto della normativa privacy (GDPR) • Verifica dell'adeguatezza delle misure di sicurezza dei dati personali • Supporto nella gestione di data breach • Raccordo con il Garante Privacy
Personale Incaricato di Elevata Qualificazione	• Applicazione delle policy di sicurezza nella propria area • Classificazione dei dati e delle informazioni gestite • Richiesta e validazione degli accessi per il proprio personale • Segnalazione tempestiva di incidenti o anomalie
Personale dell'Ente	• Utilizzo corretto e consapevole degli strumenti informatici • Rispetto delle policy e delle procedure di sicurezza • Custodia delle credenziali e dei dispositivi assegnati • Segnalazione immediata di eventi sospetti o incidenti • Partecipazione alle iniziative formative sulla sicurezza

6.2 Rapporti con l'Agenzia per la Cybersicurezza Nazionale (ACN)

L'Agenzia garantisce il rispetto degli obblighi di cooperazione e comunicazione verso l'Agenzia per la Cybersicurezza Nazionale secondo quanto previsto dalla normativa vigente, in particolare per quanto riguarda:

- Notifica tempestiva degli incidenti informatici significativi (entro le tempistiche previste dalla normativa NIS2)
- Trasmissione di report periodici sullo stato della sicurezza ICT dell'Ente
- Partecipazione a esercitazioni e simulazioni di crisi cyber
- Recepimento di direttive, raccomandazioni e allerte emesse da ACN

- Collaborazione per attività di vulnerability assessment e penetration testing coordinate a livello nazionale

Il Referente per la Sicurezza ICT è il punto di contatto designato per le comunicazioni con ACN e con le altre autorità competenti in materia di cybersicurezza.

6.3 Rapporti con fornitori e partner tecnologici

Il modello di governance tiene conto del ruolo dei fornitori, dei partner tecnologici e dei soggetti terzi che concorrono alla gestione dei sistemi informativi dell'Ente, prevedendo:

- Definizione di requisiti di sicurezza nelle specifiche tecniche e nei capitolati d'appalto
- Inserimento di clausole contrattuali in materia di sicurezza, riservatezza e gestione degli incidenti
- Verifiche periodiche sull'adeguatezza delle misure di sicurezza adottate dai fornitori
- Gestione della sicurezza della supply chain ICT (valutazione rischi di terze parti)
- Meccanismi di escalation e reporting per incidenti che coinvolgono sistemi gestiti da terzi

Resta ferma la responsabilità dell'Ente in ordine alla corretta vigilanza sull'adeguatezza delle misure di sicurezza adottate dai soggetti che trattano dati o gestiscono sistemi per conto dell'Agenzia, nei limiti e secondo le modalità previste dall'art. 28 GDPR e dalla normativa vigente.

7. Gestione del rischio informatico

L'Agenzia adotta un approccio strutturato e sistematico alla gestione del rischio informatico, inteso quale processo volto a identificare, valutare e trattare i rischi che possono incidere sulla sicurezza dei sistemi informativi, sulla continuità dei servizi digitali e sulla tutela dei dati trattati nell'esercizio delle funzioni istituzionali.

7.1 Metodologia di risk assessment

La gestione del rischio si sviluppa secondo il ciclo di vita del rischio (risk management lifecycle) articolato nelle seguenti fasi:

- **Identificazione degli asset:** Censimento dei sistemi informativi, delle infrastrutture, dei dati e dei processi critici per l'Ente
- **Analisi delle minacce:** Individuazione delle possibili fonti di danno (malware, ransomware, phishing, accessi non autorizzati, errori umani, guasti hardware, disaster naturali)
- **Valutazione delle vulnerabilità:** Identificazione dei punti deboli organizzativi e tecnologici che possono essere sfruttati dalle minacce
- **Stima dell'impatto:** Valutazione delle conseguenze operative, legali, reputazionali ed economiche di eventuali incidenti
- **Determinazione del livello di rischio:** Calcolo del rischio in termini di probabilità di accadimento e gravità dell'impatto (scala: basso / medio / alto / critico)
- **Trattamento del rischio:** Scelta delle strategie di risposta (mitigazione, trasferimento, accettazione, eliminazione)
- **Monitoraggio e riesame:** Verifica periodica dell'efficacia delle misure adottate e aggiornamento dell'analisi

L'Agenzia si avvale di metodologie riconosciute a livello nazionale e internazionale quali:

- ISO/IEC 27005 - Information security risk management
- ISO 31000 - Risk management guidelines

- NIST Special Publication 800-30 - Guide for Conducting Risk Assessments
- Framework Nazionale per la Cybersecurity e Data Protection dell'ACN

7.2 Periodicità e responsabilità

L'Agenzia provvede a:

- Condurre un'analisi del rischio informatico completa con periodicità almeno annuale
- Aggiornare la valutazione in occasione di modifiche significative dell'assetto tecnologico o organizzativo
- Rivedere l'analisi a seguito di incidenti rilevanti o di evoluzioni normative
- Documentare formalmente i risultati dell'analisi e le decisioni assunte in merito al trattamento dei rischi

La responsabilità dell'attività di risk assessment è attribuita al Referente per la Sicurezza ICT, con il supporto dell'Ufficio Sistemi Informativi e il coinvolgimento dei Responsabili di Ufficio per l'identificazione degli asset e la valutazione degli impatti.

7.3 Principali aree di rischio identificate

Sulla base delle analisi condotte, l'Agenzia ha individuato le seguenti aree prioritarie di esposizione al rischio informatico:

- **Attacchi cyber esterni:** Ransomware, phishing, DDoS, malware, exploit di vulnerabilità note
- **Perdita o furto di dati:** Data breach, accessi non autorizzati, esfiltrazione di informazioni sensibili
- **Interruzione dei servizi:** Guasti hardware, errori di configurazione, disservizi di fornitori critici
- **Errore umano:** Cancellazione accidentale di dati, configurazioni errate, violazioni involontarie di policy
- **Rischi della supply chain:** Compromissione di fornitori, backdoor in software di terze parti
- **Obsolescenza tecnologica:** Sistemi legacy non più supportati, mancanza di aggiornamenti di sicurezza

Per ciascuna area di rischio, l'Ente definisce specifiche misure di mitigazione tecniche e organizzative, documentate nelle policy e procedure operative di dettaglio.

8. Misure di sicurezza tecniche e organizzative

Sulla base dell'analisi del rischio e in conformità alle disposizioni normative vigenti (GDPR art. 32, Circolare AgID n. 1/2017, Direttiva NIS2), l'Agenzia adotta le seguenti categorie di misure di sicurezza:

8.1 Controllo degli accessi e gestione delle identità

- Autenticazione forte (MFA/2FA) per accessi a sistemi critici e accessi remoti
- Gestione centralizzata delle identità digitali (Identity and Access Management)
- Principio del least privilege: assegnazione dei privilegi minimi necessari
- Revisione periodica delle utenze e revoca tempestiva degli accessi per personale cessato
- Policy di complessità e rotazione delle password
- Segregazione degli account amministrativi da quelli operativi

8.2 Protezione della rete e segmentazione

- Firewall perimetrali e interni per la segmentazione della rete

- Sistemi di Intrusion Detection/Prevention (IDS/IPS)
- VPN per l'accesso remoto sicuro ai sistemi interni
- Filtri antispam e antiphishing su posta elettronica
- DNS filtering per blocco di domini malevoli
- Isolamento di reti WiFi guest dalla rete aziendale

8.3 Protezione degli endpoint

- Antivirus/antimalware su tutte le postazioni di lavoro e server
- Patch management: aggiornamenti tempestivi di sistema operativo e applicazioni
- Crittografia dei dischi su laptop e dispositivi mobili (BitLocker, FileVault)
- Mobile Device Management (MDM) per la gestione dei dispositivi mobili aziendali
- Politiche di screen lock automatico dopo periodo di inattività
- Divieto di installazione software non autorizzato (application whitelisting)

8.4 Protezione dei dati

- Classificazione dei dati secondo livelli di riservatezza (pubblico, interno, riservato, strettamente riservato)
- Crittografia dei dati sensibili at rest e in transit (TLS/SSL, AES-256)
- Data Loss Prevention (DLP) per prevenire fughe di informazioni
- Pseudonimizzazione e anonimizzazione dove applicabile
- Procedure di cancellazione sicura per dismissione dispositivi e supporti

8.5 Backup e disaster recovery

- Backup automatizzato con regola 3-2-1: 3 copie, 2 supporti diversi, 1 copia offsite
- Backup giornaliero incrementale e settimanale completo
- Test periodici di ripristino (almeno semestrale)
- Crittografia dei backup e protezione con autenticazione
- Piano di Disaster Recovery e Business Continuity documentato e testato
- Definizione di Recovery Time Objective (RTO) e Recovery Point Objective (RPO) per sistemi critici

8.6 Monitoraggio e logging

- Logging centralizzato degli eventi di sicurezza (SIEM - Security Information and Event Management)
- Retention dei log per almeno 12 mesi o secondo normativa applicabile
- Monitoraggio continuo H24 delle infrastrutture critiche
- Alerting automatico per eventi sospetti o anomalie
- Vulnerability assessment periodico (almeno trimestrale)
- Penetration testing annuale condotto da soggetti qualificati

8.7 Misure organizzative

- Definizione di policy e procedure operative standard (SOP)
- Formazione continua del personale su tematiche di cybersecurity
- Campagne di sensibilizzazione su phishing e social engineering
- Clausole di riservatezza e sicurezza nei contratti di lavoro

- Gestione del ciclo di vita del personale (onboarding/offboarding)
- Audit e verifiche periodiche di conformità alle policy interne

Le misure sopra elencate sono soggette a continuo aggiornamento in relazione all'evoluzione delle minacce, delle tecnologie disponibili e delle risorse dell'Ente. L'attuazione concreta di ciascuna misura è dettagliata in specifiche policy e procedure operative.

9. Gestione degli incidenti di sicurezza informatica

L'Agenzia adotta procedure strutturate per la gestione degli incidenti di sicurezza informatica, intesi quale qualsiasi evento che comprometta o minacci di compromettere la riservatezza, l'integrità o la disponibilità dei sistemi informativi e dei dati trattati.

9.1 Processo di gestione degli incidenti

Il processo di gestione degli incidenti si articola nelle seguenti fasi, disciplinate nel dettaglio dall'apposito Manuale di gestione degli incidenti di sicurezza informatica:

- **Rilevazione:** Identificazione dell'evento anomalo attraverso sistemi di monitoraggio, segnalazioni utenti o alert automatici
- **Classificazione:** Valutazione della gravità dell'incidente secondo criteri predefiniti (basso/medio/alto/critico)
- **Contenimento:** Adozione di misure immediate per limitare la diffusione e l'impatto dell'incidente
- **Eradicazione:** Eliminazione della causa root dell'incidente
- **Ripristino:** Riattivazione dei servizi e verifica del corretto funzionamento
- **Post-incident review:** Analisi delle cause, documentazione delle lesson learned, identificazione di azioni correttive

9.2 Classificazione degli incidenti

Gli incidenti sono classificati secondo i seguenti livelli di gravità:

Livello	Tempi di risposta	Esempi
CRITICO	Immediata (< 1 ora)	Ransomware, data breach massivo, compromissione server critici, indisponibilità prolungata servizi essenziali
ALTO	< 4 ore	Malware su più postazioni, accesso non autorizzato a dati sensibili, attacco DDoS parziale
MEDIO	< 24 ore	Malware su singola postazione, tentativo di phishing sventato, vulnerabilità identificata su sistema non critico
BASSO	< 72 ore	Email di spam ricevuta, rilevazione di software obsoleto, evento anomalo senza impatto

9.3 Obblighi di notifica

In presenza di incidenti che rientrino nelle fattispecie previste dalla normativa vigente, l'Agenzia assicura il rispetto degli obblighi di comunicazione nei confronti delle autorità competenti:

- **Agenzia per la Cybersicurezza Nazionale (ACN):** Notifica entro 24 ore dalla scoperta di incidenti significativi ai sensi della Direttiva NIS2
- **Garante per la Protezione dei Dati Personali:** Notifica entro 72 ore in caso di data breach che comporti rischio per i diritti e libertà degli interessati (art. 33 GDPR)
- **Interessati:** Comunicazione senza ingiustificato ritardo in caso di data breach con rischio elevato (art. 34 GDPR)

Il Referente per la Sicurezza ICT coordina le comunicazioni istituzionali, con il supporto del DPO per gli aspetti privacy.

9.4 Documentazione e registro incidenti

Tutti gli incidenti di sicurezza sono documentati in un registro centralizzato che include:

- Data e ora di rilevazione
- Tipologia e gravità dell'incidente
- Sistemi e dati coinvolti
- Azioni intraprese e tempi di risoluzione
- Cause root identificate
- Lesson learned e azioni correttive implementate

Il registro è revisionato periodicamente per identificare trend, vulnerabilità ricorrenti e aree di miglioramento.

10. Formazione e consapevolezza

L'Agenzia riconosce la formazione e la diffusione della consapevolezza in materia di sicurezza informatica quali componenti essenziali del proprio assetto organizzativo e strumenti necessari per garantire l'effettiva attuazione delle misure di sicurezza adottate.

10.1 Programma formativo

L'Ente promuove un programma strutturato di formazione articolato su:

- **Formazione di base (obbligatoria per tutto il personale):**

- Principi di sicurezza informatica e protezione dei dati
- Riconoscimento di phishing e social engineering
- Gestione sicura delle password
- Uso corretto di dispositivi e servizi aziendali

- **Formazione specialistica (personale ICT e ruoli chiave):**

- Gestione avanzata della sicurezza ICT
- Incident response e forensics
- Secure coding e security by design

- **Aggiornamenti periodici:** Sessioni di refresher almeno annuali per mantenere alto il livello di consapevolezza

- **Campagne di sensibilizzazione:** Comunicazioni mirate su nuove minacce, allerte di sicurezza, best practice

10.2 Modalità e tempistiche

La formazione è erogata attraverso:

- Corsi e-learning su piattaforma LMS (Learning Management System)
- Webinar e sessioni in aula
- Simulazioni di attacchi phishing (phishing simulation test)
- Materiale informativo e guide operative
- Newsletter periodiche sulla sicurezza

Tempistiche:

- Formazione di base: entro 90 giorni dall'assunzione o prima dell'assegnazione delle credenziali di accesso
- Aggiornamenti: con periodicità almeno annuale
- Formazione specialistica: pianificazione annuale con identificazione dei fabbisogni formativi

La partecipazione alla formazione obbligatoria è tracciata e rendicontata annualmente. L'Ente monitora l'efficacia delle attività formative attraverso test di verifica e analisi dei risultati delle simulazioni di phishing.

11. Miglioramento continuo e aggiornamento del documento

Il sistema di governance della sicurezza informatica dell'Agenzia è improntato al principio del miglioramento continuo, inteso quale costante adeguamento dell'assetto organizzativo e delle misure adottate rispetto all'evoluzione del contesto normativo, tecnologico e organizzativo.

11.1 Ciclo Plan-Do-Check-Act

L'Agenzia adotta il ciclo PDCA (Plan-Do-Check-Act) come modello di miglioramento continuo:

- **Plan:** Definizione di obiettivi, policy e procedure; pianificazione delle attività di risk assessment
- **Do:** Implementazione delle misure di sicurezza; erogazione della formazione; gestione operativa
- **Check:** Monitoraggio, audit interni ed esterni, vulnerability assessment, analisi degli incidenti
- **Act:** Azioni correttive, aggiornamento di policy e procedure, revisione dell'analisi del rischio

11.2 Attività di verifica

L'Ente pianifica le seguenti attività di verifica:

- Audit interno annuale sul sistema di gestione della sicurezza
- Vulnerability assessment sulle infrastrutture critiche
- Penetration test condotto da soggetti esterni qualificati
- Simulazioni di phishing periodiche (almeno 2 campagne all'anno)
- Test di disaster recovery
- Riesame annuale dell'analisi del rischio ICT

11.3 Revisione del documento

Il presente documento è soggetto a revisione in caso di:

- Modifiche rilevanti del quadro normativo
- Innovazioni tecnologiche significative
- Cambiamenti organizzativi rilevanti
- Incidenti gravi che evidenzino lacune nell'assetto di sicurezza
- Risultanze di audit o valutazioni esterne che richiedano adeguamenti

Gli aggiornamenti sono adottati secondo le procedure interne dell'Agenzia, previa approvazione degli Organi competenti, e sono comunicati a tutto il personale interessato.

12. Coordinamento con altri atti e documenti

Il presente documento si coordina e si integra con i seguenti atti e documenti dell'Agenzia:

- **Regolamento per l'utilizzo degli strumenti informatici** - Norme comportamentali per l'uso corretto di dispositivi, email, internet, software
- **Manuale di gestione degli incidenti di sicurezza informatica** - Procedure operative dettagliate per rilevazione, gestione e ripristino
- **Registro dei trattamenti (art. 30 GDPR)** - Mappatura dei dati personali trattati e relative misure di sicurezza
- **Piano Triennale per l'Informatica** - Programmazione degli investimenti e progetti ICT

Le disposizioni contenute nel presente documento devono essere interpretate in modo coerente con il quadro normativo vigente e con gli altri atti organizzativi dell'Ente, secondo un principio di sistematicità e coordinamento tra le diverse fonti interne.

Per quanto non espressamente disciplinato, restano fermi gli obblighi e le disposizioni previsti dalla normativa europea e nazionale applicabile, nonché gli ulteriori obblighi settoriali eventualmente pertinenti.