Ente di gestione delle aree protette dei Parchi Reali

***Sede legale**: viale C. Emanuele II, 256 – 10078 Venaria Reale (TO) – tel. 011 4320980*
***Sede operativa di Stupinigi**: viale Torino 4, (fraz. Stupinigi) – 10042 Nichelino (TO) – tel. 011 3587575*
partita IVA e codice fiscale 01699930010
http://www.parchireali.it – email: protocollo@parchireali.to.it – parchireali@legalmail.it

PIANO DI GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA

Anno 2026

Sommario

1. INTRODUZIONE

La sicurezza informatica rappresenta un elemento essenziale per garantire la continuità operativa, la protezione delle informazioni e la resilienza dell'Ente. Incidenti di sicurezza, come attacchi informatici, ransomware o attacchi DDoS, possono determinare impatti significativi sulle attività istituzionali e sui servizi offerti, sia in termini operativi sia reputazionali.

La gestione degli incidenti – intesa come l'insieme delle attività volte a rilevare tempestivamente un evento, a rispondervi in modo appropriato ed efficiente, a ripristinare la situazione pre-incidente e a migliorare la capacità di risposta futura – costituisce una capacità determinante per la sicurezza dell'Ente.

Per gestire efficacemente gli incidenti, è cruciale adottare un approccio strutturato basato su processi e procedure chiaramente definiti, creando un quadro organizzativo armonizzato che assicuri coerenza e sistematicità delle attività. La definizione di processi e procedure consente inoltre di garantire ripetibilità, facilitare la formazione del personale e apprendere dalle lezioni degli eventi passati.

Il presente Piano di Gestione degli Incidenti Informatici disciplina l'insieme delle azioni "reattive" del sistema di sicurezza ICT dell'Ente, integrandosi con il **Piano della Sicurezza Informatica e Analisi dei Rischi** e le **Disposizioni operative in materia di incidenti di sicurezza e di violazione di dati personali (c.d. DATA BREACH)**.

Tuttavia, **non tutti gli incidenti informatici comportano necessariamente una violazione di dati personali** ai sensi della normativa in materia di protezione dei dati: un incidente può infatti riguardare un malfunzionamento tecnico, un'interruzione di servizio, un attacco non andato a buon fine o una compromissione circoscritta che non determini alcuna perdita, distruzione, divulgazione o accesso non autorizzato a dati personali. Solo laddove l'evento integri i presupposti di una violazione dei dati personali, trova applicazione il **Piano Data Breach**. I due Piani operano pertanto in modo coordinato ma autonomo. Il presente Piano quindi **non sostituisce né replica le disposizioni del Piano Data Breach, al quale si rinvia integralmente per ogni aspetto relativo alla protezione dei dati personali.**

1.2 Finalità del documento

Il documento fornisce linee guida per la definizione di processi e procedure volti a gestire in modo efficace gli incidenti di sicurezza informatica nell'Ente, in conformità al **Codice dell'Amministrazione Digitale (CAD, d.lgs. 82/2005)** e alle linee guida dell'**Agenzia per la Cybersicurezza Nazionale** adottate con Decreto ACN n.344695 del 30/10/2025.

1.3 Obiettivi principali:

- Definire responsabilità, ruoli e flussi decisionali nella gestione degli incidenti;
- Delineare le fasi operative di rilevazione, analisi, contenimento, ripristino e post-evento;
- Coordinare le attività del personale interno e dei fornitori ICT;
- Garantire la tracciabilità e documentazione delle azioni intraprese;
- Favorire il miglioramento continuo tramite analisi post-evento.

1.4 Contesto normativo

NORMA	DESCRIZIONE
Codice dell'Amministrazione Digitale – CAD	Decreto legislativo 7 marzo 2005, n. 82. Normativa di riferimento per le PA.
Perimetro di Sicurezza Nazionale Cibernetica (PSNC)	Decreto-legge 21 settembre 2019, n. 105. Disposizioni urgenti sulla sicurezza nazionale cibernetica.
Legge 90/2024	Legge 28 giugno 2024, n. 90. Rafforzamento della cybersicurezza nazionale e dei reati informatici.
Regolamento Cloud per la PA	Decreto Direttoriale ACN n. 21007/24 del 27 giugno 2024. Disposizioni sul cloud della PA.
Decreto NIS	Decreto legislativo 4 settembre 2024, n. 138. Recepimento direttiva UE 2022/2555 su cibersicurezza.
Linee guida dell'Agenzia per la Cybersicurezza Nazionale	Decreto ACN n.344695 del 30/10/2025

1.5 Contesto operativo dell'Ente

L'Ente opera nell'ambito delle proprie funzioni istituzionali mediante l'utilizzo di sistemi informativi, infrastrutture digitali e piattaforme applicative a supporto dei processi amministrativi, gestionali e tecnici.

Il patrimonio informativo dell'Ente – comprensivo dei dati istituzionali, amministrativi e personali trattati nello svolgimento delle attività – è oggetto di specifica classificazione, analisi e valutazione nell'ambito del **Piano della Sicurezza Informatica e Analisi dei Rischi**.

All'interno di tale Piano sono descritte:

- le misure di sicurezza organizzative, fisiche e logiche adottate;
- le ulteriori misure da adottare in funzione del livello di rischio rilevato;
- i criteri di valutazione delle minacce e delle vulnerabilità;
- le azioni di mitigazione e miglioramento.

Il Piano della Sicurezza Informatica e Analisi dei Rischi, è oggetto di aggiornamento con cadenza almeno annuale, nonché ogniqualvolta intervengano modifiche significative:

- nell'infrastruttura tecnologica;
- nell'assetto organizzativo;
- nei trattamenti di dati personali;
- nel quadro normativo di riferimento;
- nello scenario delle minacce.

Il presente Piano di Gestione degli Incidenti si colloca in continuità con tale documento e disciplina la componente reattiva del sistema di sicurezza, definendo le modalità organizzative e operative da attivare in caso di evento rilevante per la sicurezza o incidente informatico.

1.6 Termini e definizioni

TERMINE	DEFINIZIONE
Evento	Qualsiasi accadimento osservabile in una rete o sistema informativo.
Evento rilevante per la sicurezza	Evento di natura intenzionale o accidentale che potrebbe compromettere o compromette la sicurezza dei sistemi informativi e di rete, in termini di disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi.

TERMINE	DEFINIZIONE
Falso positivo	Allarme segnalato da uno strumento di monitoraggio che non corrisponde a un incidente.
Gestione degli incidenti di sicurezza informatica	Insieme di processi e procedure volti a prevenire, rilevare, analizzare, contenere un incidente di sicurezza, rispondere e recuperare da esso.
Incidente di sicurezza informatica	Evento che compromette la disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi offerti dai sistemi informatici e di rete.
Indicatore di compromissione (IOC)	Informazione che descrive una minaccia o compromissione nota.
Minaccia informatica	Qualsiasi circostanza, evento o azione che potrebbe danneggiare o avere un impatto negativo su reti, sistemi informativi, utenti o altre persone.
Sistema informativo e di rete	Dispositivo o insieme di dispositivi interconnessi che eseguono un trattamento automatico di dati digitali, comprese le reti e i dati conservati, elaborati o trasmessi.
Tattiche, Tecniche, Procedure (TTPs)	Obiettivi e modalità di azione di un attore malevolo durante le fasi di un attacco informatico.
Vulnerabilità	Punto debole o difetto di prodotti ICT o servizi ICT che può essere sfruttato da una minaccia informatica.

2. AMBITO DI APPLICAZIONE

2.1 Principio di proporzionalità

L'applicazione del presente Piano avviene secondo il principio di proporzionalità, tenendo conto:

- della gravità dell'evento;
- dell'impatto sui servizi;
- del numero di sistemi coinvolti;
- della natura dei dati trattati;
- della durata dell'interruzione.

Non ogni malfunzionamento costituisce un incidente di sicurezza rilevante; tuttavia, ogni evento potenzialmente significativo deve essere valutato secondo i criteri definiti nel Capitolo 3.

2.2 Perimetro tecnologico

Il presente Piano si applica a tutti i sistemi informativi, alle infrastrutture tecnologiche e ai servizi digitali utilizzati dall'Ente per lo svolgimento delle proprie funzioni istituzionali, come individuati nel Piano della Sicurezza Informatica e nell'Analisi dei Rischi.

Rientrano nel perimetro:

- infrastrutture di rete e sicurezza;
- server e ambienti virtualizzati;
- postazioni di lavoro e dispositivi mobili aziendali;
- applicativi gestionali e sistemi documentali;
- servizi erogati in modalità cloud.

Il Piano si applica agli eventi che possano compromettere disponibilità, integrità, riservatezza o continuità operativa.

2.3 Perimetro organizzativo

Il presente Piano si applica a tutto il personale che, a qualunque titolo, utilizzi o gestisca sistemi informativi dell'Ente.

Sono destinatari delle disposizioni:

- personale dipendente;
- amministratori di sistema;
- collaboratori e consulenti autorizzati;
- soggetti esterni che operano sui sistemi in virtù di rapporti contrattuali.

Ogni soggetto che accede ai sistemi informativi dell'Ente ha l'obbligo di segnalare tempestivamente eventuali anomalie o eventi sospetti.

La gestione operativa dell'incidente è affidata alle figure individuate nel modello di governance del presente Piano, ma la responsabilità di collaborazione e segnalazione è diffusa nell'intera organizzazione.

La sicurezza informatica è intesa come responsabilità organizzativa condivisa e non esclusivamente tecnica.

2.4 Servizi digitali critici

Ai fini del presente Piano assumono particolare rilevanza i servizi digitali considerati essenziali per il funzionamento dell'Ente o per l'erogazione dei servizi ai cittadini.

Sono considerati critici i servizi che:

- supportano attività obbligatorie per legge;
- garantiscono funzioni amministrative essenziali;
- trattano dati personali in misura significativa;
- consentono l'accesso ai servizi digitali da parte dell'utenza esterna;
- assicurano la gestione documentale e la protocollazione ufficiale.

In caso di incidente che coinvolga uno o più servizi critici, il livello di risposta organizzativa può essere elevato, prevedendo priorità nel ripristino, informazione alla Direzione e attivazione del coordinamento rafforzato.

L'elenco dei servizi critici è coerente con l'analisi dei rischi contenuta nel Piano della Sicurezza Informatica dell'Ente ed è soggetto ad aggiornamento periodico.

3. DEFINIZIONE E CLASSIFICAZIONE DEGLI INCIDENTI INFORMATICI

Come indicato al cap.1.6 un **incidente di sicurezza informatica** è qualsiasi evento che compromette la disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi offerti dai sistemi informatici e di rete dell'Ente.

Distinzione concettuale:

- **Evento/Anomalia:** problema tecnico isolato, senza impatto significativo sui servizi o sui dati.
- **Incidente:** evento che produce o può produrre impatto reale o potenziale su servizi, dati, processi o obblighi normativi.

Tutti gli incidenti devono essere registrati nel **Registro Incidenti dell'Ente (All.A)**, indipendentemente dall'impatto immediato.

3.1 Tipologie di incidenti informatici

L'Ente identifica le seguenti tipologie di incidenti informatici rilevanti ai fini della continuità operativa, della sicurezza delle informazioni e della protezione dei dati personali. Le categorie individuate consentono una classificazione omogenea degli eventi e l'attivazione delle procedure di gestione previste.

a. **Incidenti di sicurezza informatica (Cybersecurity)**

Rientrano in tale categoria gli eventi derivanti da azioni dolose, interne o esterne, volte a compromettere riservatezza, integrità o disponibilità delle informazioni e dei sistemi:

- **Malware e Ransomware:** infezioni da software malevolo finalizzate alla cifratura, sottrazione o distruzione di dati, nonché al blocco dei sistemi informativi.
- **Phishing e compromissione delle credenziali:** accessi non autorizzati conseguenti a furto di credenziali, attacchi di social engineering o compromissione di account istituzionali.
- **Accessi non autorizzati e intrusioni:** tentativi o accessi indebiti ai sistemi informativi, sia da parte di soggetti esterni sia interni.
- **Attacchi DoS/DDoS:** saturazione delle risorse di rete o dei servizi esposti con conseguente indisponibilità degli stessi.
- **Exploit di vulnerabilità (incluse zero-day):** sfruttamento di vulnerabilità note o non ancora pubblicamente documentate.
- **Minacce interne (insider threat):** comportamenti dolosi o gravemente negligenti da parte di personale interno o collaboratori con accesso ai sistemi.
- **Manipolazione o alterazione non autorizzata dei dati:** modifiche indebite a informazioni, registri o documenti ufficiali.

b. **Incidenti tecnologici e operativi**

Eventi derivanti da malfunzionamenti, errori umani o criticità tecniche:

- **Errori operativi o configurazioni errate:** modifiche non corrette a sistemi, applicativi o configurazioni di rete che generano disservizi o vulnerabilità.
- **Interruzioni di servizio:** indisponibilità di server, applicativi critici o servizi digitali essenziali.
- **Vulnerabilità critiche non sanate:** mancata applicazione di aggiornamenti di sicurezza che espongono i sistemi a rischio elevato.
- **Guasti hardware o software:** malfunzionamenti di infrastrutture, apparati di rete, sistemi di storage o piattaforme applicative.

c. **Incidenti con impatto sui dati personali**

Eventi che comportano una violazione dei dati personali trattati dall'Ente e che richiedono l'attivazione delle procedure previste dal **Piano di Data Breach**:

- Accesso, divulgazione o perdita non autorizzata di dati personali
- Distruzione o alterazione accidentale o illecita di dati personali
- Furto o smarrimento di dispositivi contenenti dati personali

d. Incidenti fisici e ambientali con impatto ICT

Eventi di natura non strettamente informatica ma con effetti sui sistemi e sui dati:

- Incendio, allagamento o eventi naturali
- Blackout prolungati o guasti agli impianti elettrici
- Furto o danneggiamento di apparecchiature ICT

e. Incidenti relativi a fornitori e servizi esternalizzati

Eventi riconducibili a soggetti terzi che erogano servizi ICT o infrastrutturali:

- **Incidenti su servizi cloud o SaaS:** interruzioni, malfunzionamenti o compromissioni presso fornitori esterni.
- **Compromissione della supply chain ICT:** vulnerabilità o aggiornamenti software compromessi che impattano i sistemi dell'Ente.
- **Inadempienze contrattuali con impatto sulla sicurezza o disponibilità dei servizi.**

Per maggiori approfondimenti sugli incidenti dei servizi cloud, consultare il **Cap. 4 'Incidenti relativi a servizi erogati in modalità cloud'."**

Nota metodologica: la classificazione sopra riportata non è esaustiva ma rappresenta un quadro di riferimento operativo. Ogni evento che comprometta o possa compromettere la riservatezza, l'integrità o la disponibilità delle informazioni o dei sistemi informativi dell'Ente è da considerarsi incidente informatico e deve essere gestito secondo le procedure previste dal presente Piano.

3.2 Classificazione degli incidenti per livello di gravità

Gli incidenti informatici sono classificati in base all'impatto su riservatezza, integrità, disponibilità (CIA), continuità operativa, impatto economico, reputazionale e normativo.

Livelli di gravità

Livello	Descrizione	Impatto operativo	Esempi
Basso	Evento circoscritto, facilmente contenibile, senza impatti su dati personali o servizi critici	Disservizio limitato e temporaneo	Malware su singola postazione isolata
Medio	Impatto su più utenti o sistemi non critici	Riduzione parziale dell'operatività	Interruzione temporanea di servizio non essenziale
Alto	Compromissione di sistemi critici o possibile violazione dati personali	Interruzione significativa di servizi istituzionali	Ransomware su server dipartimentale
Critico	Impatto esteso su infrastrutture core o violazione massiva di dati personali	Blocco totale dei servizi essenziali o grave danno reputazionale	Attacco ransomware generalizzato, data breach su larga scala

Criteri di valutazione

Un incidente è classificato considerando:

- Numero di utenti coinvolti

- Tipologia di dati impattati (ordinari, particolari, giudiziari)
- Durata dell'interruzione
- Impatto economico stimato
- Obblighi di notifica normativa
- Impatto reputazionale

La classificazione può essere aggiornata nel corso della gestione dell'incidente.

3.3 Obblighi di notifica e tempistiche

Le tempistiche di notifica sono determinate dalla normativa applicabile e dalla gravità dell'incidente.

Livello	Notifica interna	Notifica esterna	Es. tipologia incidente
Basso / Medio	Entro 4 ore al Responsabile Sistema informativo	Non prevista, salvo evoluzione dell'incidente	Malware senza impatto su dati personali né servizi critici
Alto	Immediata (entro 1 ora) a Responsabile Sistema informativo e Direzione	Se incidente significativo ai sensi NIS2: pre-notifica entro 24 ore all'autorità competente	Interruzione di servizio critico
Alto / Critico	Immediata al DPO e al Titolare del trattamento	Entro 72 ore al Garante per la protezione dei dati personali ai sensi del Regolamento (UE) 2016/679; comunicazione agli interessati se rischio elevato	Violazione di dati personali (Data Breach)
Alto / Critico	Immediata a Direzione, Responsabile Sistema informativo	Early warning entro 24 ore; notifica dettagliata entro 72 ore; relazione finale entro 1 mese ai sensi della Direttiva (UE) 2022/2555	Incidente significativo ai sensi NIS2
Medio / Alto	Entro 4 ore al Responsabile Sistema informativo e alla Funzione contratti	Secondo obblighi contrattuali; se impatto significativo, notifica ai sensi NIS2	Incidente su fornitore ICT critico

Precisazioni operative:

- La notifica interna è sempre obbligatoria, anche in assenza di obblighi esterni;
- La classificazione dell'incidente può evolvere nel tempo, modificando gli obblighi di notifica;
- In caso di sovrapposizione normativa (es. Data Breach + incidente NIS2), si applicano entrambe le procedure di notifica;
- Tutti gli incidenti devono essere registrati nel Registro degli Incidenti..

4. INCIDENTI RELATIVI A SERVIZI ICT EROGATI DA FORNITORI ESTERNI (INCLUSI SERVIZI IN MODALITÀ CLOUD)

L'Ente si avvale, per l'erogazione di alcuni servizi, di fornitori esterni che operano sia in modalità cloud sia attraverso altre forme di fornitura di servizi ICT (quali manutenzione, assistenza, gestione di sistemi applicativi o infrastrutturali). Le previsioni del presente capitolo si applicano a tutte le tipologie di fornitura di servizi informatici esternalizzati, indipendentemente dalla modalità tecnica di erogazione.

In tali casi si distingue tra:

- responsabilità tecnica dell'infrastruttura, in capo al fornitore;
- responsabilità istituzionale e organizzativa, in capo all'Ente.

Il ricorso a servizi ICT erogati da fornitori esterni, indipendentemente dalla modalità tecnica di fornitura (cloud o altra forma di esternalizzazione), non comporta il trasferimento della responsabilità dell'Ente in materia di sicurezza, continuità operativa e protezione dei dati.

4.1 Ripartizione delle responsabilità

Se l'incidente riguarda l'infrastruttura tecnica del fornitore (es. indisponibilità del servizio, attacco ai sistemi cloud, malfunzionamenti del data center):

- il fornitore gestisce gli aspetti tecnici e il ripristino del servizio;
- l'Ente valuta l'impatto organizzativo e attiva le proprie procedure interne.

Se l'incidente deriva da utilizzo improprio, errore interno o compromissione di credenziali dell'Ente:

- la gestione è principalmente in capo all'Ente;
- il fornitore fornisce supporto tecnico.

In ogni caso:

- l'evento deve essere registrato nel Registro degli Incidenti dell'Ente;
- la classificazione e le decisioni organizzative spettano all'Ente;
- eventuali obblighi normativi restano in capo all'Ente.

4.2 Coordinamento con gli accordi contrattuali

Gli aspetti contrattuali relativi alla sicurezza ICT, ai livelli di servizio, alla continuità operativa, alla protezione dei dati personali e al monitoraggio delle forniture sono disciplinati nei contratti ICT dell'Ente come da Piano di Procurement ICT vigente.

Il Piano di Procurement ICT definisce i principi, le responsabilità e le azioni operative volte a garantire che l'acquisizione e la gestione dei servizi e delle soluzioni informatiche avvengano nel rispetto delle disposizioni normative, delle linee guida nazionali e delle misure di sicurezza previste dal Piano della Sicurezza Informatica e Analisi dei Rischi dell'Ente. In tale ambito sono previsti requisiti di sicurezza, clausole specifiche nei documenti di gara, attività di audit, monitoraggio dei fornitori e verifiche periodiche.

Il presente Piano di Gestione degli Incidenti opera in coerenza con tale disciplina e ne rappresenta il complemento operativo per la fase di risposta agli eventi di sicurezza.

In particolare, nei contratti relativi a servizi ICT — ivi inclusi i servizi erogati in modalità cloud nonché ogni altra forma di fornitura di servizi informatici esternalizzati — e con specifico riguardo ai sistemi classificati come critici, devono essere previsti:

- obblighi di tempestiva comunicazione all'Ente di incidenti di sicurezza, vulnerabilità gravi o malfunzionamenti che possano incidere sulla disponibilità, integrità o riservatezza dei sistemi e dei dati;

- livelli minimi di servizio (SLA) e tempi di ripristino coerenti con le esigenze di continuità operativa dell'Ente;

- obblighi di collaborazione tecnica nella gestione degli eventi di sicurezza;

- disponibilità delle informazioni e delle evidenze tecniche necessarie alla valutazione dell'incidente (log, report tecnici, informazioni sull'impatto e sulle misure adottate);

- facoltà per l'Ente di effettuare verifiche, controlli o audit in relazione agli eventi occorsi durante l'esecuzione del contratto.

Inoltre ove il fornitore tratti dati personali per conto dell'Ente, i contratti devono altresì includere l'**accordo sul trattamento dei dati personali (c.d. nomina a responsabile del trattamento) ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (GDPR)**, che costituisce parte integrante della disciplina contrattuale ai fini del presente Piano.

La gestione tecnica dell'incidente da parte del fornitore non comporta il trasferimento della responsabilità istituzionale dell'Ente, che resta titolare della classificazione dell'evento, della valutazione dell'impatto organizzativo e dell'adempimento degli eventuali obblighi normativi, ivi inclusi quelli in materia di protezione dei dati personali.

La disciplina contrattuale costituisce pertanto uno strumento di regolazione dei rapporti con i fornitori, ma non sostituisce né limita le responsabilità dell'Ente nella governance complessiva della sicurezza informatica e nella gestione degli incidenti.

4.3 Clausola contrattuale fornitori – Gestione degli incidenti di sicurezza

In coerenza con:

- il Codice dell'Amministrazione Digitale (art. 51 – sicurezza e continuità);
- il Regolamento Generale sulla Protezione dei Dati (artt. 28, 32, 33 – sicurezza e data breach);
- le linee guida in materia di sicurezza ICT per le PA;
- Piano di Procurement ICT dell'Ente;

di seguito la clausola da inserire nei contratti dei servizi erogati in modalità cloud:

Art. X – Gestione degli incidenti di sicurezza, classificazione e obblighi di notifica

2. Il Fornitore si impegna ad adottare misure tecniche e organizzative adeguate a garantire la sicurezza, la disponibilità, l'integrità e la riservatezza dei sistemi e dei dati trattati per conto dell'Ente, in coerenza con la normativa vigente e con le disposizioni interne dell'Amministrazione.
3. Il Fornitore è tenuto a comunicare all'Ente, senza ingiustificato ritardo, qualsiasi incidente di sicurezza, vulnerabilità grave, malfunzionamento critico o evento che possa compromettere:
    - la disponibilità dei servizi erogati;
    - l'integrità dei dati;
    - la riservatezza delle informazioni;
    - la continuità operativa dell'Ente.
4. Ai fini contrattuali, gli incidenti sono classificati secondo i seguenti livelli di severità:

    a) Incidente Critico: evento che comporta interruzione totale di un servizio essenziale, compromissione significativa di dati o potenziale data breach rilevante. **Tempo massimo di notifica: entro 4 ore dalla conoscenza dell'evento.**

    b) Incidente Alto: evento che determina grave degrado di un servizio critico o rischio significativo per i dati, senza interruzione totale. **Tempo massimo di notifica: entro 8 ore dalla conoscenza dell'evento.**

c) Incidente Medio: evento con impatto limitato e circoscritto su sistemi o utenti, senza effetti strutturali sui servizi. **Tempo massimo di notifica: entro 24 ore dalla conoscenza dell'evento.**

d) Incidente Basso: anomalia tecnica o evento minore senza impatto significativo su servizi o dati.**Comunicazione entro 3 giorni lavorativi o nel report periodico di sicurezza.**

5. La prima classificazione può essere proposta dal Fornitore, ma la classificazione definitiva dell'incidente ai fini organizzativi e istituzionali spetta esclusivamente all'Ente.
6. La comunicazione di cui al presente articolo deve contenere almeno:
   - descrizione dell'evento;
   - data e ora di rilevazione;
   - sistemi e servizi coinvolti;
   - misure di contenimento adottate;
   - valutazione preliminare dell'impatto;
   - tempi stimati di ripristino.
7. Il Fornitore si impegna a collaborare attivamente nella gestione dell'incidente, fornendo tempestivamente log, evidenze tecniche, report di analisi e ogni informazione utile alla valutazione dell'evento e agli eventuali adempimenti normativi dell'Ente.
8. La gestione tecnica dell'incidente da parte del Fornitore non comporta il trasferimento della responsabilità istituzionale dell'Ente, che resta titolare della valutazione dell'impatto organizzativo, della classificazione finale e degli eventuali obblighi normativi, inclusi quelli in materia di protezione dei dati personali.
9. L'Ente si riserva la facoltà di effettuare verifiche, audit o richieste di chiarimento in relazione agli incidenti occorsi durante l'esecuzione del contratto.

5. PROCESSO DI GESTIONE DEGLI INCIDENTI

5.1 Modello di riferimento

Il processo di gestione degli incidenti dell'Ente è strutturato secondo il modello metodologico indicato dalle Linee Guida dell'Agenzia per la Cybersicurezza Nazionale e sulla base di quello riportato nel documento NIST *Incident Response Recommendations and Considerations for Cybersecurity Risk Management SP 800-61r3*, articolato nelle seguenti macro-fasi:

1. Preparazione
2. Rilevamento
3. Risposta
4. Ripristino e Miglioramento

Le fasi costituiscono un ciclo continuo e integrato, finalizzato a garantire resilienza organizzativa e miglioramento progressivo delle capacità di risposta.

Il modello adottato recepisce gli obiettivi organizzativi e operativi indicati nell'Appendice A delle Linee Guida ACN, già integrati nelle finalità e negli obiettivi del presente Piano.

5.2 Preparazione

La fase di Preparazione comprende l'insieme delle misure organizzative, procedurali e tecniche che l'Ente adotta per garantire la capacità di prevenire, individuare e gestire efficacemente un incidente informatico.

In coerenza con il modello indicato dalle Linee Guida dell'Agenzia per la Cybersicurezza Nazionale, la fase di preparazione si articola nelle seguenti componenti: Governo, Identificazione e Protezione.

5.2.1 Governo

In questa sotto-fase è definito il quadro strategico e organizzativo per la gestione degli incidenti, come, ad esempio, l'elaborazione di politiche per la gestione degli incidenti di sicurezza e l'assegnazione di ruoli e responsabilità.

Matrice RACI del Processo di Gestione degli Incidenti

La matrice di assegnazione responsabilità (cosiddetta matrice RACI) permette di definire chiaramente ruoli e responsabilità per le varie attività di un processo:

- **Responsible (R):** chi esegue operativamente l'attività.
- **Accountable (A):** chi ha la responsabilità sul risultato dell'attività.
- **Consulted (C):** chi viene consultato durante l'esecuzione dell'attività in quanto possiede conoscenze necessarie al completamento dell'attività.
- **Informed (I):** chi è informato sull'avanzamento e il completamento dell'attività.

I ruoli del processo di gestione degli incidenti sono associati alle nomine interne dell'Ente secondo quanto riportato nella tabella sottostante.

Le responsabilità operative e decisionali sono attribuite secondo il modello RACI adottato nel presente Piano, garantendo per ciascuna attività la presenza di almeno un Responsible (R) e di un unico Accountable (A), in conformità alle Linee Guida ACN.

Associazione Ruoli al Modello RACI

Ruolo Linee Guida ACN	Nomina Interna Associata	Ruolo prevalente nel modello RACI	Ambito di Responsabilità nel Processo
Organizzazione per la Sicurezza Informatica	Responsabile della Transizione Digitale (RTD)	A	Governo strategico, approvazione Piano, supervisione miglioramento
Responsabile della Gestione dell'Incidente	Responsabile dei Sistemi Informativi	A nelle fasi operative	Coordinamento tecnico, gestione risposta, supervisione ripristino
IRT (Incident Response Team) / Funzione Tecnica di Risposta	Amministratore di Sistema	R	Monitoraggio, analisi tecnica, contenimento, eradicazione, ripristino
SOC (Security Operation Center)	Amministratore di Sistema / Resp. Sistemi Informativi	R / C	Analisi eventi di sicurezza, supporto monitoraggio
Ufficio IT	Responsabile dei	C / R	Gestione infrastruttura, supporto

Ruolo Linee Guida ACN	Nomina Interna Associata	Ruolo prevalente nel modello RACI	Ambito di Responsabilità nel Processo
	Sistemi Informativi		tecnico
Ufficio Legale	DPO	A per obblighi privacy	Valutazione obblighi normativi, notifiche data breach, consulenza legale
Ufficio Comunicazione / URP	URP / Comunicazione	C / I	Supporto nella comunicazione esterna / interna, interfaccia con cittadini e stampa
Gestione Documentale / Conservazione	Responsabile Protocollo Informatico e Conservazione	R / C	Protocollazione, tracciabilità, gestione comunicazioni ufficiali interne, conservazione evidenze digitali

Tabella RACI – Gestione degli Incidenti

Fase	Attività	Responsabile Protocollo Informatico e Conservazione	URP / Comunicazione	RTD	Resp. Sistemi Informativi	DPO	Amministratore di Sistema
Preparazione – Governo	Definizione politiche e Piano	C	I	A	R	C	C
Preparazione – Governo	Definizione criteri classificazione	C	I	A	R	C	C
Preparazione – Governo	Definizione flussi di escalation e notifica	C	I	A	R	C	C
Preparazione – Identificazione	Identificazione asset critici	C	I	C	A	C	R
Preparazione – Identificazione	Mappatura trattamenti dati personali	C	I	C	R	A	C
Preparazione – Protezione	Implementazione misure tecniche di sicurezza	I	I	C	A	C	R
Preparazione – Protezione	Gestione backup e protezione dati	I	I	C	A	C	R
Preparazione – Protezione	Formazione e sensibilizzazione	C	I	A	R	C	I
Rilevamento	Monitoraggio eventi di sicurezza	I	I	I	A	I	R
Rilevamento	Analisi preliminare evento	I	I	C	A	C	R

Fase	Attività	Responsabile Protocollo Informatico e Conservazione	URP / Comunicazione	RTD	Resp. Sistemi Informativi	DPO	Amministratore di Sistema
Rilevamento	Apertura e classificazione incidente	C	I	C	A	C	R
Risposta – Investigazione	Analisi tecnica approfondita	I	I	C	A	C	R
Risposta – Investigazione	Raccolta evidenze digitali	R	I	C	A	C	R
Risposta – Notifica	Valutazione obbligo notifica GDPR	I	C	C	C	A	R
Risposta – Notifica	Notifica al Garante Privacy	R	C	C	C	A	C
Risposta – Notifica	Comunicazioni istituzionali interne	R	C	A	C	C	I
Risposta – Contenimento	Contenimento tecnico incidente	I	I	C	A	I	R
Risposta – Contenimento	Misure temporanee di mitigazione	I	I	C	A	I	R
Risposta – Eradicazione	Rimozione causa radice	I	I	C	A	I	R
Risposta – Eradicazione	Validazione sicurezza post-eradicazione	I	I	C	A	C	R
Ripristino	Ripristino sistemi e servizi	I	I	C	A	I	R
Ripristino	Verifica integrità dati e archivi	R	I	C	A	C	C
Miglioramento	Post Incident Review	C	I	A	R	C	C
Miglioramento	Aggiornamento misure di sicurezza	I	I	C	A	C	R
Miglioramento	Aggiornamento del Piano	C	I	A	R	C	C

5.2.2 Identificazione

In questa sotto-fase è acquisita la componente di Identificazione dell'attività sistematica di conoscenza e presidio degli elementi che possono essere oggetto di compromissione.

Tali attività comprendono:

- censimento e aggiornamento dell'infrastruttura tecnologica;
- individuazione dei servizi digitali critici;
- analisi delle minacce e delle vulnerabilità;
- valutazione del rischio informatico;
- mappatura delle dipendenze tecnologiche (incluse quelle relative a servizi cloud e fornitori esterni).

L'Ente disciplina tali aspetti nel **Piano della Sicurezza Informatica e Analisi dei Rischi**, che contiene:

- la descrizione del sistema informatico;
- l'inventario degli apparati e delle infrastrutture;
- l'analisi delle minacce e delle vulnerabilità;
- la matrice dei rischi ICT;
- le misure di mitigazione adottate.

Il presente Piano non riproduce tali contenuti, ma li assume quale base conoscitiva indispensabile per:

- valutare l'impatto di un incidente;
- determinare il livello di severità;
- individuare le priorità di intervento;
- stabilire le modalità di ripristino.

5.2.3 Protezione

La sotto-fase di *Protezione* comprende l'insieme delle misure tecniche, organizzative e procedurali adottate dall'Ente per ridurre la probabilità che un incidente si verifichi e per limitarne l'impatto qualora si manifesti.

La Protezione non coincide con la gestione dell'incidente, ma rappresenta il presupposto operativo che consente di:

- contenere più rapidamente gli effetti di un evento dannoso;
- preservare l'integrità delle evidenze;
- assicurare la continuità dei servizi essenziali;
- ridurre l'esposizione al rischio.

Le misure di protezione sono disciplinate in modo analitico nel **Piano della Sicurezza Informatica e Analisi dei Rischi**, cui il presente documento rinvia. In questa sede si richiamano esclusivamente gli elementi rilevanti ai fini della gestione degli incidenti.

Misure tecniche di protezione

Le misure tecniche adottate dall'Ente comprendono, in via generale:

- sistemi di protezione perimetrale (firewall, segmentazione di rete);
- sistemi antivirus e antimalware aggiornati;
- sistemi di autenticazione e gestione delle credenziali;
- sistemi di backup periodico dei dati;
- aggiornamento regolare dei sistemi e delle applicazioni;
- protezione degli accessi ai servizi cloud;

- monitoraggio dei log e delle attività di sistema.

Tali misure non eliminano il rischio di incidente, ma ne riducono la probabilità e ne circoscrivono gli effetti.

La loro configurazione e gestione operativa è affidata al Responsabile dei Sistemi Informativi e ai fornitori ICT, secondo le responsabilità definite nei capitoli precedenti.

Misure organizzative e procedurali

Accanto alle misure tecniche, l'Ente adotta misure organizzative finalizzate a prevenire comportamenti a rischio e a rafforzare la resilienza complessiva del sistema informativo.

Rientrano in tale ambito:

- politiche interne sull'utilizzo degli strumenti informatici;
- regolamentazione delle credenziali di accesso;
- procedure di attivazione e disattivazione degli account;
- separazione dei ruoli amministrativi;
- controllo sugli accessi privilegiati;
- formazione periodica del personale.

La consapevolezza del personale costituisce uno degli strumenti più efficaci di protezione, in quanto numerosi incidenti derivano da errori umani, distrazione o scarsa attenzione a segnali di rischio (es. phishing).

Backup e continuità operativa

Elemento centrale della fase di Protezione è la disponibilità di copie di sicurezza affidabili e periodicamente verificate.

L'Ente garantisce:

- l'esecuzione regolare dei backup dei dati critici;
- la separazione logica o fisica delle copie di sicurezza rispetto ai sistemi principali;
- la verifica periodica della possibilità di ripristino;
- la definizione delle priorità di recupero dei servizi.

Le modalità operative sono disciplinate nel **Piano della Sicurezza Informatica e analisi dei rischi** e negli accordi con i fornitori ICT, in particolare per i servizi erogati in modalità cloud.

La disponibilità di backup verificati costituisce presupposto essenziale per la gestione di incidenti quali ransomware o perdita accidentale di dati.

Protezione nei servizi ICT erogati da fornitori esterni

Per i servizi erogati tramite fornitori esterni, le misure di protezione sono attuate in parte dal fornitore e in parte dall'Ente.

La protezione nei servizi si realizza pertanto attraverso un modello di responsabilità condivisa come indicato al **cap.4 Incidenti relative a servizi ICT erogati da fornitori esterni (inclusi servizi i mdalità cloud).**

5.3 Rilevamento

La fase di rilevamento ha la finalità di individuare tempestivamente eventi che possano compromettere la sicurezza dei sistemi informativi, dei servizi digitali e delle informazioni trattate dall'Ente.

Il rilevamento non si esaurisce nella mera generazione di segnalazioni tecniche, ma costituisce una funzione strutturata e continuativa, finalizzata a:

- intercettare anomalie rilevanti;
- distinguere tra evento tecnico e incidente;
- attivare, ove necessario, il processo di gestione;
- garantire tracciabilità e accountability.

In coerenza con le Linee Guida nazionali, la capacità di rilevamento è parte integrante del sistema complessivo di gestione della sicurezza informatica e si fonda sull'integrazione tra strumenti tecnologici, analisi del rischio e assetto organizzativo.

La fase di rilevamento prevede due tipologie di attività:

- **Rilevazione proattiva**
  monitoraggio continuo e analisi periodica dei sistemi, finalizzata a individuare anomalie anche non segnalate dagli utenti.

- **Rilevazione reattiva**
  attivata in seguito a segnalazioni da parte di utenti, tecnici o sistemi automatizzati, che richiedono l'avvio di verifiche più approfondite.

In entrambi i casi, la rilevazione non si limita alla constatazione dell'evento, ma comprende:

- la raccolta delle informazioni disponibili;
- la verifica della veridicità dell'allarme;
- l'iniziale definizione del perimetro dell'incidente.

5.3.1 Capacità di monitoraggio e fonti di rilevazione

L'Ente dispone di strumenti di monitoraggio automatico integrati nell'infrastruttura ICT (quali sistemi antivirus, firewall, sistemi di logging e strumenti di controllo degli accessi), idonei a generare segnalazioni in presenza di anomalie o comportamenti potenzialmente rilevanti ai fini della sicurezza.

Le caratteristiche tecniche e le modalità di configurazione di tali strumenti sono disciplinate nel **Piano della Sicurezza Informatica e Analisi dei Rischi**, cui il presente Piano rinvia per quanto attiene agli aspetti di prevenzione e protezione.

Il rilevamento può avvenire attraverso una pluralità di fonti, tra cui ad esempio:

- sistemi automatici di protezione e monitoraggio;
- analisi delle informazioni registrate nei log di sistema;
- segnalazioni del personale interno;
- comunicazioni dei fornitori ICT, in particolare per servizi erogati in modalità cloud;
- informazioni provenienti da fonti istituzionali competenti in materia di cybersicurezza.

La pluralità delle fonti consente di rafforzare la capacità di intercettazione degli eventi e di ridurre il rischio di mancata individuazione di situazioni critiche.

5.3.2 Logiche di rilevamento adottate

In coerenza con le metodologie indicate dalle Linee Guida nazionali, l'Ente adotta logiche di rilevamento fondate su modelli complementari, proporzionati alla propria dimensione organizzativa e al contesto tecnologico di riferimento.

a) Rilevamento basato su Indicatori di Compromissione (IOC-based)

Il sistema di rilevamento si avvale dell'individuazione di segnali noti di compromissione, quali alert generati dagli strumenti di sicurezza, segnalazioni relative a componenti malevoli o comunicazioni con indirizzi riconosciuti come potenzialmente dannosi.

Tale modalità consente di intercettare minacce già conosciute e codificate nei sistemi di protezione.

b) Rilevamento basato su anomalie (Anomaly-based)

L'Ente considera rilevanti anche comportamenti anomali rispetto al normale funzionamento dei sistemi o dei servizi digitali, quali variazioni inattese nei modelli di accesso, utilizzo o traffico.

L'analisi delle anomalie permette di individuare eventi che, pur non corrispondendo a minacce già note, possono costituire indicatori di rischio.

c) Rilevamento basato su schemi di attacco (TTP-based)

Il processo di rilevamento tiene conto, in modo proporzionato, di tecniche e modalità di attacco comunemente note, anche sulla base di segnalazioni e aggiornamenti provenienti da fornitori ICT o da fonti istituzionali.

In relazione alla dimensione dell'Ente, tale modalità si realizza principalmente attraverso l'aggiornamento continuo dei sistemi di sicurezza e il coordinamento con i soggetti tecnici responsabili della gestione dell'infrastruttura.

5.3.3 Adeguamento e tuning delle logiche di rilevamento

Il sistema di rilevamento non è statico, ma è oggetto di periodica verifica e aggiornamento.

In particolare, sono oggetto di revisione:

- le soglie di attivazione degli alert;
- gli indicatori di compromissione utilizzati;
- le configurazioni dei sistemi di monitoraggio;
- la qualità e la rilevanza delle segnalazioni generate.

L'obiettivo del tuning è:

- ridurre i falsi positivi;
- evitare la sottovalutazione di eventi effettivamente critici;
- adeguare il sistema alle evoluzioni del contesto tecnologico e delle minacce.

Le attività di aggiornamento tecnico sono svolte dall'Amministratore di Sistema in collaborazione con il Responsabile dei Sistemi Informativi o dal fornitore ICT, nell'ambito delle misure di sicurezza disciplinate dal **Piano della Sicurezza Informatica e Analisi dei Rischi**.

5.3.4 Distinzione tra evento e incidente

Non ogni anomalia costituisce un incidente.

Il rilevamento determina l'emersione di un evento di sicurezza, che viene successivamente valutato alla luce dei criteri di classificazione definiti nel Capitolo 3 del presente Piano.

Solo qualora l'evento presenti un impatto effettivo o potenziale su disponibilità, integrità o riservatezza dei sistemi o dei dati, esso è qualificato come incidente e si passa alla successiva fase di Risposta.

5.3.5 Tracciabilità della fase di rilevamento

Gli eventi rilevati e ritenuti meritevoli di approfondimento sono oggetto di registrazione secondo le modalità previste nel sistema di gestione degli incidenti dell'Ente.

La registrazione garantisce:

- tracciabilità delle decisioni;
- ricostruibilità delle valutazioni effettuate;
- supporto alle eventuali attività di audit o verifica.

5.4 Risposta

La sotto-fase di *Risposta* – costituita dalle sotto-fasi di *investigazione, notifica, contenimento ed eradicazione* - ha la finalità di gestire l'incidente in modo coordinato, proporzionato e documentato, limitandone l'impatto sui sistemi informativi, sui servizi digitali e sui dati trattati dall'Ente.

La risposta si fonda sui seguenti principi:

- proporzionalità rispetto alla gravità dell'incidente;
- tempestività nelle decisioni e nelle azioni;
- tracciabilità delle attività svolte;
- coordinamento tra funzioni interne e fornitori ICT;
- integrazione con il Piano Data Breach, ove applicabile.

La gestione della risposta non è esclusivamente tecnica, ma organizzativa e decisionale.

5.4.1 Investigazione

La fase di investigazione costituisce il momento di approfondimento analitico dell'incidente, successivo alla sua individuazione e classificazione preliminare.

L'obiettivo dell'investigazione non è esclusivamente tecnico, ma organizzativo e decisionale: essa consente all'Ente di comprendere con sufficiente chiarezza la natura dell'evento, le sue cause, l'estensione dell'impatto e le possibili evoluzioni, al fine di adottare misure di contenimento ed eradicazione adeguate e proporzionate.

L'attività investigativa si sviluppa attraverso la raccolta e l'analisi delle informazioni disponibili, tra cui ad esempio:

- evidenze tecniche ricavate dai sistemi coinvolti;
- registrazioni dei log;
- informazioni fornite dagli strumenti di monitoraggio;
- eventuali segnalazioni del personale o dei fornitori ICT.

L'analisi è orientata a ricostruire la sequenza temporale dell'evento, individuando il punto di origine, le modalità di propagazione e i sistemi interessati.

Nel caso in cui l'incidente coinvolga servizi erogati in modalità cloud o infrastrutture gestite da fornitori esterni, l'investigazione si svolge in coordinamento con il soggetto tecnico competente, nel rispetto delle responsabilità definite contrattualmente. (cap.4 incidenti relativi a servizi erogati in modalità cloud).

Durante tale fase deve essere garantita, per quanto possibile, la preservazione delle evidenze utili alla ricostruzione dei fatti, evitando interventi che possano alterare in modo irreversibile le informazioni necessarie all'analisi.

Le modalità operative di raccolta delle evidenze sono disciplinate nel **Manuale SOP (Standard Operating Procedure) allegato al presente Piano (All.B).**

In coerenza con le Linee Guida nazionali per la gestione degli incidenti, l'investigazione comprende anche la caratterizzazione dell'evento secondo la **tassonomia cyber dell'Agenzia per la Cybersicurezza Nazionale (ACN)** pubblicata all'indirizzo https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn

L'adozione della tassonomia ACN non sostituisce la classificazione interna per livelli di severità (Critico, Alto, Medio, Basso) prevista nel Capitolo 3 del presente Piano, ma la integra, consentendo una lettura dell'evento sia in termini di impatto organizzativo sia in termini di tipologia tecnica.

In questo modo, l'Ente assicura coerenza metodologica con il quadro nazionale di riferimento e facilita l'eventuale interlocuzione con autorità competenti.

Al termine dell'investigazione preliminare, devono risultare chiariti, per quanto possibile:

- l'origine dell'incidente;
- l'estensione del perimetro coinvolto;
- l'eventuale compromissione di dati personali o informazioni critiche;
- il livello di gravità effettivo;
- le azioni necessarie per il contenimento e l'eradicazione.

Qualora, nel corso dell'analisi, emergano elementi che configurino una violazione di dati personali, si procede secondo quanto previsto nel **Piano Data Breach** dell'Ente, attivando il coinvolgimento del DPO.

L'investigazione può proseguire anche nelle fasi successive alla stabilizzazione dell'evento, al fine di approfondire le cause radice (root cause analysis) e individuare eventuali misure correttive strutturali.

5.4.2 Notifica

La fase di notifica costituisce parte integrante della risposta all'incidente e si attiva a seguito della classificazione preliminare dell'evento effettuata nella fase di investigazione.

La notifica non rappresenta un mero adempimento formale, ma uno strumento di governo dell'incidente, finalizzato a garantire:

- consapevolezza organizzativa;
- attivazione dei livelli decisionali appropriati;
- rispetto degli obblighi normativi applicabili;

- coordinamento con eventuali soggetti esterni coinvolti.

Le tempistiche e i livelli di notifica sono disciplinati nel Capitolo 3.3 del presente Piano, al quale si rinvia integralmente.

Comunicazione interna

La notifica interna è sempre obbligatoria, indipendentemente dalla gravità dell'evento.

Essa consente di:

- informare tempestivamente il Responsabile Sistemi Informativi;
- coinvolgere la Direzione nei casi di maggiore impatto;
- attivare il DPO nei casi in cui vi sia anche solo il sospetto di una violazione di dati personali;
- coordinare eventuali azioni con l'area amministrativa o contrattuale.

La classificazione dell'incidente può evolvere nel corso dell'investigazione.
Qualora emergano nuovi elementi, il livello di notifica viene aggiornato di conseguenza.

Obblighi normativi applicabili

Alla data di adozione del presente Piano, l'Ente non rientra tra i soggetti obbligati ai sensi della Direttiva (UE) 2022/2555 (NIS2), in quanto non eroga servizi qualificabili come essenziali o importanti secondo la normativa vigente. Pertanto, non sussiste un obbligo generalizzato di notifica al CSIRT Italia.
Eventuali comunicazioni al CSIRT possono essere effettuate su base volontaria, qualora ritenuto opportuno in funzione della gravità o della natura dell'evento, ed è anzi raccomandabile farlo in presenza di incidenti di rilievo, anche al fine di contribuire alla condivisione delle informazioni sulle minacce a livello nazionale.

N.B. Evoluzione normativa — Obbligo di notifica in caso di ransomware

Si segnala che è in corso di approvazione parlamentare il disegno di legge in materia di reati informatici e rafforzamento della cybersicurezza nazionale **(A.S. 1441)**, il quale prevede, tra l'altro, l'introduzione di un **obbligo di notifica al CSIRT Italia entro sei ore dalla conoscenza dell'evento per tutti i soggetti pubblici vittime di un attacco ransomware, indipendentemente dall'assoggettamento alla disciplina NIS2.**
In considerazione di tale evoluzione normativa, e in applicazione del principio di precauzione, l'Ente adotta fin d'ora la seguente procedura operativa in caso di incidente ransomware:

- il Responsabile dei Sistemi Informativi valuta tempestivamente la natura dell'evento e, qualora vi siano evidenze o fondato sospetto di un attacco ransomware, informa senza ritardo il Responsabile della Transizione Digitale;
- entro sei ore dalla conoscenza dell'evento, viene effettuata — su base volontaria e in anticipazione del futuro obbligo normativo — una comunicazione al CSIRT Italia attraverso i canali ufficiali disponibili sul portale dell'Agenzia per la Cybersicurezza Nazionale;
- la comunicazione è documentata nel Registro degli Incidenti.

All'entrata in vigore della nuova disciplina, la presente procedura acquisterà valore di adempimento obbligatorio senza necessità di modifiche operative al Piano.

Protezione dei dati personali

Resta pienamente applicabile la normativa in materia di protezione dei dati personali. Qualora l'incidente integri una violazione di dati personali, si attivano le procedure previste dal **Piano Data Breach** dell'Ente, con eventuale notifica all'Autorità Garante per la protezione dei dati personali nei termini previsti dal Regolamento (UE) 2016/679.

In caso di sovrapposizione tra diverse fattispecie normative, le relative procedure si applicano cumulativamente.

Notifica nei casi di coinvolgimento di fornitori ICT

Qualora l'incidente coinvolga servizi o infrastrutture erogati da fornitori ICT, si applicano le disposizioni di cui al Capitolo 4 del presente Piano.

In particolare:

- restano ferme le regole sulla ripartizione delle responsabilità tra Ente e fornitore;
- si applicano gli obblighi contrattuali di comunicazione e collaborazione tecnica;
- si applicano i livelli di severità e le relative tempistiche contrattuali già disciplinate.

La gestione tecnica dell'incidente da parte del fornitore non modifica né attenua la responsabilità istituzionale dell'Ente, che conserva:

- la classificazione finale dell'evento ai fini organizzativi;
- la valutazione dell'impatto sui servizi e sulle attività istituzionali;
- l'adempimento degli eventuali obblighi normativi.

La presente sezione non introduce ulteriori obblighi rispetto a quelli già previsti nel Capitolo 4, ma ne richiama l'applicazione nella fase di risposta all'incidente.

Comunicazione esterna

La gestione della notifica e delle comunicazioni connesse all'incidente si ispira ai seguenti principi:

- proporzionalità rispetto alla gravità dell'evento;
- accuratezza delle informazioni trasmesse;
- tracciabilità delle comunicazioni effettuate;
- tutela della riservatezza delle informazioni sensibili;
- centralizzazione delle comunicazioni esterne nei casi di maggiore rilevanza.

La comunicazione esterna, ove necessaria, è coordinata dalla Direzione in raccordo con il Responsabile dei Sistemi Informativi e, se coinvolti dati personali, con il DPO.

5.4.3 Contenimento

La fase di contenimento si attiva a seguito della caratterizzazione preliminare dell'incidente ed è finalizzata a limitare l'estensione dell'evento, ridurne l'impatto sui servizi e prevenire ulteriori compromissioni.

Essa rappresenta una fase cruciale del processo di risposta, in quanto incide direttamente sulla continuità operativa dell'Ente e sulla stabilità dei sistemi informativi.

Il contenimento deve essere proporzionato alla gravità dell'incidente, coerente con la classificazione effettuata e attuato nel rispetto dei principi di tracciabilità e preservazione delle evidenze.

Contenimento immediato (Short-Term Containment)

Il contenimento immediato ha carattere tempestivo e mira a interrompere la propagazione dell'evento nel minor tempo possibile.

In questa fase possono essere adottate misure quali ad esempio:

- isolamento logico di sistemi o account compromessi;
- disattivazione temporanea di credenziali;
- segmentazione o restrizione del traffico di rete;
- sospensione temporanea di servizi digitali.

Le decisioni devono essere coordinate dal Responsabile dei Sistemi Informativi, tenendo conto:

- dell'urgenza dell'evento;
- dell'impatto organizzativo;
- dell'eventuale necessità di coinvolgere la Direzione nei casi di servizi rilevanti.

Le azioni di contenimento non devono compromettere la raccolta delle evidenze utili all'investigazione, né alterare in modo irreversibile lo stato dei sistemi senza adeguata documentazione.

Contenimento strutturale (Long-Term Containment)

Successivamente alla fase immediata, può rendersi necessario adottare misure di contenimento strutturale, finalizzate a stabilizzare l'ambiente tecnologico in attesa dell'eradicazione completa della causa dell'incidente.

Tali misure possono includere ad esempio:

- rafforzamento temporaneo delle configurazioni di sicurezza;
- monitoraggio intensificato dei sistemi coinvolti;
- attivazione di controlli aggiuntivi di autenticazione;
- limitazioni temporanee su funzionalità non essenziali.

Il contenimento strutturale ha lo scopo di mantenere l'incidente sotto controllo evitando recrudescenze o ulteriori compromissioni.

Bilanciamento tra sicurezza e continuità operativa

Le Linee Guida in materia di gestione degli incidenti evidenziano la necessità di bilanciare l'esigenza di neutralizzare la minaccia con quella di garantire la continuità dei servizi.

Nel caso in cui il contenimento comporti:

- interruzione di servizi digitali;
- limitazione di funzionalità rilevanti;
- impatti sull'utenza interna o esterna;

la decisione deve essere adeguatamente motivata e registrata nel **Registro degli Incidenti.**

Il principio guida è la riduzione del rischio complessivo per l'Ente, valutando sia l'impatto della minaccia sia l'impatto delle misure adottate.

Coinvolgimento di fornitori ICT

Qualora l'incidente coinvolga servizi erogati da fornitori esterni, il contenimento tecnico può essere effettuato dal fornitore, nel rispetto delle disposizioni di cui al Capitolo 4.

Valutazione del rischio residuo

Prima di procedere alla fase di eradicazione, deve essere effettuata una valutazione del rischio residuo, volta ad accertare:

- l'assenza di propagazioni ulteriori;
- la stabilità dei sistemi isolati;
- la sostenibilità operativa delle misure adottate.

La valutazione del rischio residuo costituisce elemento di collegamento tra contenimento ed eradicazione e deve essere adeguatamente documentata.

5.5 Eradicazione

La sotto-fase di *Eradicazione* si attiva a seguito del contenimento dell'incidente e ha l'obiettivo di rimuovere definitivamente la causa tecnica che ha reso possibile l'evento, eliminando vulnerabilità, componenti malevole, configurazioni insicure o condizioni di esposizione.

Se il contenimento limita l'impatto immediato, l'eradicazione mira a prevenire la reiterazione dell'incidente e a ripristinare un livello di sicurezza adeguato e stabile.

L'eradicazione deve essere condotta sulla base delle risultanze dell'investigazione e della caratterizzazione dell'incidente effettuata secondo la tassonomia di riferimento.

Analisi della causa radice (Root Cause Analysis)

Prima di procedere alla rimozione definitiva delle componenti compromesse, deve essere effettuata un'analisi della causa radice dell'incidente.

Tale analisi è finalizzata a individuare:

- la vulnerabilità sfruttata;
- il vettore di attacco o la modalità di compromissione;
- eventuali carenze organizzative o procedurali;
- configurazioni errate o misure di sicurezza insufficienti.

L'eradicazione non può limitarsi alla rimozione degli effetti visibili dell'incidente, ma deve intervenire sulle condizioni che ne hanno consentito l'insorgenza.

La causa radice identificata deve essere documentata nel **Registro degli Incidenti.**

Rimozione della compromissione

Sulla base dell'analisi effettuata, vengono adottate misure tecniche volte ad esempio a:

- eliminare malware, backdoor o strumenti di accesso non autorizzati;
- rimuovere account compromessi o privilegi non appropriati;
- correggere vulnerabilità mediante aggiornamenti o patch;
- ripristinare configurazioni sicure dei sistemi.

L'attività tecnica è svolta dall'Amministratore di Sistema, sotto il coordinamento del Responsabile dei Sistemi Informativi.

Qualora siano coinvolti fornitori ICT, l'eradicazione tecnica può essere effettuata dal fornitore, ferma restando la supervisione e validazione da parte dell'Ente.

Eliminazione delle persistenze e verifica di integrità

Le Linee Guida evidenziano la necessità di accertare che l'attaccante o la causa tecnica dell'incidente non mantenga elementi di persistenza all'interno dell'infrastruttura.

Devono pertanto essere effettuate verifiche volte ad accertare:

- l'assenza di accessi residui non autorizzati;
- l'assenza di componenti malevole latenti;
- la coerenza delle configurazioni con le politiche di sicurezza vigenti.

Solo a seguito di tali verifiche può considerarsi completata la fase di eradicazione.

Rafforzamento delle misure di sicurezza (Hardening)

L'eradicazione costituisce anche un momento di rafforzamento complessivo del sistema di sicurezza.

In funzione delle criticità emerse, possono essere adottate misure quali:

- revisione delle politiche di accesso;
- rafforzamento delle configurazioni di sicurezza;
- introduzione di controlli aggiuntivi;
- aggiornamento delle procedure interne;
- intensificazione temporanea del monitoraggio.

Tali interventi devono essere proporzionati alla gravità dell'incidente e integrati nel **Piano della Sicurezza Informatica e Analisi dei Rischi.**

Coordinamento con il DPO e con eventuali obblighi normativi

Nel caso in cui l'incidente abbia comportato una violazione di dati personali, la fase di eradicazione si coordina con le indicazioni fornite dal DPO nell'ambito del **Piano Data Breach**.

Collegamento con il ciclo di miglioramento

Le criticità emerse durante l'eradicazione devono essere oggetto di valutazione ai fini:

- dell'aggiornamento dell'analisi dei rischi;
- della revisione delle misure tecniche e organizzative;
- dell'eventuale aggiornamento del presente Piano;
- della pianificazione di attività formative o di sensibilizzazione.

In tal modo, l'eradicazione non rappresenta un'attività isolata, ma si integra nel ciclo di miglioramento continuo della sicurezza informatica dell'Ente.

5.6 Ripristino e Miglioramento

La sotto-fase di *Ripristino* si attiva a seguito del completamento delle attività di contenimento ed eradicazione e ha l'obiettivo di riportare progressivamente i sistemi e i servizi alle condizioni operative ordinarie, garantendo al contempo un adeguato livello di sicurezza.

Il ripristino non coincide con la mera riattivazione tecnica dei sistemi, ma rappresenta un processo strutturato volto a ristabilire stabilità, affidabilità e continuità dei servizi istituzionali.

Finalità della fase di ripristino

La fase di ripristino è finalizzata a:

- riattivare in sicurezza i sistemi e i servizi interessati;
- verificare l'integrità e la coerenza dei dati;
- monitorare eventuali anomalie successive all'eradicazione;
- garantire la continuità operativa delle attività dell'Ente;
- ristabilire condizioni di esercizio stabili e controllate.

Il ripristino deve essere proporzionato alla gravità dell'incidente e coerente con le risultanze della fase di investigazione e di eradicazione.

Ripristino tecnico dei sistemi

Il ripristino tecnico può includere ad esempio:

- reinstallazione o riconfigurazione di sistemi compromessi;
- ripristino da backup verificati;
- riallineamento delle configurazioni di sicurezza;
- riattivazione controllata di servizi sospesi.

Prima della riattivazione completa, deve essere effettuata una verifica di integrità dei sistemi e dei dati, al fine di accertare:

- l'assenza di compromissioni residue;
- la correttezza dei dati ripristinati;
- la coerenza delle configurazioni con le politiche di sicurezza vigenti.

Le attività tecniche sono coordinate dal Responsabile dei Sistemi Informativi e svolte dall'Amministratore di Sistema.

Nel caso di servizi in modalità cloud, il ripristino tecnico può essere effettuato dal fornitore, sotto supervisione dell'Ente, in coerenza con quanto previsto nel Cap.4.

Ripristino della continuità operativa

Oltre al ripristino tecnico, la fase di recovery comprende la progressiva normalizzazione delle attività organizzative.

In particolare, devono essere valutati:

- l'impatto dell'interruzione sui procedimenti amministrativi;
- eventuali arretrati generati dall'indisponibilità dei sistemi;
- la necessità di comunicazioni integrative verso utenti interni o esterni.

Qualora l'incidente abbia inciso su servizi digitali rilevanti, il rientro alla piena operatività può avvenire in modo graduale e controllato, con monitoraggio rafforzato.

Monitoraggio post-ripristino

Le Linee Guida sottolineano l'importanza di una fase di monitoraggio successiva alla riattivazione dei sistemi.

Per un periodo proporzionato alla gravità dell'incidente, devono essere attivati:

- controlli rafforzati sugli accessi;
- verifica dei log e delle anomalie;
- monitoraggio della stabilità dei servizi.

Il monitoraggio post-ripristino ha lo scopo di intercettare tempestivamente eventuali criticità residue o recidive.

Chiusura formale dell'incidente

L'incidente può essere dichiarato formalmente chiuso quando:

- le attività di contenimento ed eradicazione sono completate;
- il ripristino tecnico è stato verificato;
- la continuità operativa è ristabilita;
- eventuali obblighi normativi sono stati adempiuti;
- la documentazione è completa e registrata.

La chiusura è formalizzata dal Responsabile dei Sistemi Informativi e annotata nel **Registro degli Incidenti.**

Lezioni apprese (*lesson learned*) e miglioramento

Al termine dell'incidente deve essere effettuata una valutazione complessiva dell'evento, volta a individuare:

- eventuali criticità organizzative o tecniche;
- margini di miglioramento nei processi;
- necessità di aggiornamento delle misure di sicurezza;
- opportunità formative per il personale.

Le risultanze devono essere considerate nell'ambito:

- dell'aggiornamento del Piano della Sicurezza Informatica e Analisi dei Rischi;
- della revisione del presente Piano;
- del processo di miglioramento continuo.

In tal modo, ogni incidente costituisce un elemento di rafforzamento del sistema di sicurezza dell'Ente.

6. FORMAZIONE

L'Ente riconosce la formazione e la sensibilizzazione del personale quale misura fondamentale per la prevenzione e la corretta gestione degli incidenti informatici, nonché per la tutela dell'integrità, riservatezza e disponibilità delle informazioni e dei sistemi informativi.

A tal fine, tutto il personale dipendente e chiunque, a qualsiasi titolo, utilizzi strumentazioni, risorse informatiche o servizi digitali dell'Ente ha ricevuto il **Disciplinare di utilizzo degli strumenti informatici dell'Ente**, pubblicato nell'apposita sezione dell'Amministrazione dell'Ente.

La presa visione del Disciplinare è accompagnata da specifiche attività formative volte ad assicurare la piena conoscenza delle regole di utilizzo delle risorse informatiche, delle misure di sicurezza adottate e delle responsabilità connesse al loro impiego.

Sono altresì messe a disposizione piattaforme formative dedicate, sia di natura privata sia ministeriale, al fine di garantire un costante aggiornamento in materia di sicurezza informatica, protezione dei dati e gestione degli incidenti.

In caso di aggiornamento delle procedure o di introduzione di nuove misure organizzative e tecniche, l'Ente provvede tempestivamente a informare e formare il personale interessato, assicurando la diffusione delle istruzioni operative da adottare e promuovendo un livello adeguato e continuo di consapevolezza in materia di sicurezza informatica.

La formazione è intesa come processo continuo e strutturato, volto a rafforzare la cultura della sicurezza e a ridurre il rischio derivante da comportamenti non conformi o inconsapevoli.

Esercitazioni e simulazioni di gestione degli incidenti

Al fine di verificare l'efficacia delle procedure previste dal presente Piano e rafforzare la capacità organizzativa di risposta agli incidenti informatici, l'Ente può programmare periodicamente esercitazioni e simulazioni di gestione degli incidenti.

Le esercitazioni hanno lo scopo di:

- verificare la corretta comprensione dei ruoli e delle responsabilità previsti dal Piano;
- testare i flussi di comunicazione interna tra le diverse funzioni coinvolte;
- valutare l'efficacia delle procedure operative e degli strumenti di risposta;
- migliorare il coordinamento tra le componenti tecniche, organizzative e amministrative coinvolte nella gestione degli incidenti;
- individuare eventuali criticità procedurali o organizzative.

Gli esiti delle esercitazioni possono essere documentati e utilizzati come elemento di miglioramento continuo delle procedure e delle misure organizzative previste dal presente Piano, anche attraverso eventuali aggiornamenti del Manuale delle Procedure Operative (SOP) e degli altri strumenti operativi collegati.

7. REVISIONE E AGGIORNAMENTO DEL PIANO

I presente Piano è soggetto a revisione periodica e ad aggiornamento sistematico, al fine di garantirne la costante adeguatezza rispetto al contesto organizzativo, tecnologico e normativo di riferimento, nonché all'evoluzione delle minacce informatiche.

8. ALLEGATI

La gestione degli incidenti informatici deve essere improntata ai principi di *tracciabilità, responsabilizzazione e trasparenza amministrativa*. Ogni evento, indipendentemente dalla sua gravità, deve essere oggetto di adeguata registrazione e documentazione, al fine di garantire la ricostruibilità delle decisioni assunte, delle azioni intraprese e delle responsabilità coinvolte.

Durante la gestione dell'incidente devono essere conservate le evidenze tecniche e documentali rilevanti, quali log di sistema, report di analisi, comunicazioni interne ed esterne, relazioni tecniche e ogni altro elemento utile alla ricostruzione dell'evento. La conservazione avviene nel rispetto delle regole interne in materia di gestione documentale e delle disposizioni sulla conservazione dei documenti informatici.

Il presente Piano è integrato da strumenti operativi che ne assicurano la concreta applicazione nell'organizzazione dell'Ente e ne supportano l'efficacia in tutte le fasi di gestione degli incidenti.

Sono adottati:

- **All.A Registro degli Incidenti:** custodito dal Responsabile dei Sistemi Informativi, nel quale sono annotati gli eventi rilevati, la classificazione attribuita, le principali fasi della gestione, le misure adottate e la data di chiusura dell'incidente. Il Registro costituisce strumento essenziale di governo, controllo e rendicontazione interna, nonché base informativa per eventuali verifiche o audit.
- **All.B Manuale delle Procedure Operative (SOP),** che disciplina in dettaglio le modalità operative di gestione degli incidenti nelle diverse fasi del processo, in piena coerenza con le disposizioni del presente Piano;
- **All.C Playbook tematici (*Ransomware, Phishing, Data Breach, Ddos, Password Spray, Rilevamento, Comunicazione, Post-incidente, Readiness operativa*):** destinati a fornire indirizzi operativi per tipologie ricorrenti o particolarmente rilevanti di incidente;
- **All.D Modulo di segnalazione dell'incidente:** volto a uniformare le modalità di comunicazione interna e a garantire la raccolta strutturata delle informazioni iniziali;
- **All.E Checklist di risposta all'incidente:** strumento di supporto operativo per verificare, nelle prime fasi di gestione, che siano attivate tutte le azioni necessarie secondo la classificazione dell'evento e la sua evoluzione.

Si segnala che la **Matrice RACI,** che formalizza ruoli e responsabilità, **è riportata nel Capitolo 5.2.1**, mentre la **clausola contrattuale per fornitori ICT è descritta nel Capitolo 4**.

L'insieme di questi strumenti garantisce coerenza applicativa, uniformità di comportamento, tracciabilità delle attività svolte e rafforza il principio di accountability che ispira il Piano, assicurando che ogni fase della gestione degli incidenti sia documentata e verificabile.

I documenti allegati al presente Piano contengono informazioni operative riservate relative alle modalità di rilevamento, risposta e ripristino in caso di incidente informatico. In quanto tali, sono classificati ad uso interno e non soggetti a pubblicazione ai sensi del D.Lgs. 33/2013 (Codice della

Trasparenza), ai sensi dell'art. 24, comma 1, lett. a) e c) della L. 241/1990, nonché in applicazione del principio di sicurezza delle informazioni previsto dall'art. 51 del D.Lgs. 82/2005 (CAD). La diffusione dei suddetti documenti è consentita esclusivamente al personale interno autorizzato e ai soggetti esterni coinvolti nella gestione degli incidenti informatici dell'Ente, nei limiti strettamente necessari all'espletamento delle relative funzioni.