Comune di Parma

PROCEDURA PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA DELLE INFORMAZIONI

Documento per approvazione formale ai fini RS.MA-01

Comune di Parma

Questo documento è confidenziale. Le informazioni confidenziali non devono essere divulgate a terze parti diverse dai dipendenti e dai fornitori autorizzati da Comune di Parma e IT.CITY con apposita autorizzazione scritta. Le terze parti autorizzate potranno solo prendere visione della versione cartacea o digitale del documento presso le sedi del Comune di Parma e di IT.CITY. Le informazioni confidenziali devono essere tenute in luogo sicuro e non devono essere riprodotte o usate per scopi non autorizzati da Comune di Parma e IT.CITY. La riproduzione può avvenire solo con l'autorizzazione del Comune di Parma e di IT.CITY e le copie devono recare la classificazione dei documenti originali.
I documenti originali sono conservati e consultabili nel repository documentale sharepoint Settore Transizione Digitale - Pagina iniziale).

Redazione, Variazioni, Approvazioni

Redazione

Autore:
Data di creazione: 14/04/2025
Ultimo aggiornamento: 03/06/2026
Codice:
Versione: 1.1
Stato:
Classificazione interno

Variazioni

Data	Autore	Versione	Variazione
03/06/2026	Settore Sviluppo Economico e Transizione Digitale	1.1	Adeguamento ISO/IEC 27001:2022 e NIS2 (D.Lgs. 138/2024)

Approvazioni

Nome	Funzione	Data	Firma
Ferioli Nicola	Dirigente Settore Sviluppo Economico e Transizione Digitale	29/06/2026	

Lista distribuzione

L'elenco delle risorse che accedono al documento è gestito. Il documento è accessibili all'interno di un repository

IT.CITY S.P.A. (Società in house, controllata – a socio unico - sottoposta all'attività di direzione e coordinamento del Comune di Parma) tramite contratto stipulato in data 23 maggio 2022 Rep. N. 19608 della Raccolta Scritture Private del Comune di Parma, maggio 2022 - aprile 2025, e rinnovato fino ad aprile 2028 mediante la stipula del contratto Rep. SP/20365/2025 del 4 luglio 2025, è stata nominata Gestore del Sistema Informatico Comunale di Parma. La presente procedura, ai sensi del Contratto sopracitato, garantisce lo sviluppo coerente e l'integrazione di nuove tecnologie nell'intero sistema informativo dell'Ente e definisce le procedure e le istruzioni sicurezza per una gestione efficace e completa.

SOMMARIO

1. INTRODUZIONE 5
2. SCOPO E CAMPO DI APPLICAZIONE 6
3. RIFERIMENTI 6
4. DEFINIZIONI 7
5. INCIDENTE DI SICUREZZA 9
6. DATA BREACH AI SENSI DEL GDPR 10
7. RUOLI E RESPONSABILITÀ 11
8. PROCEDURA DI GESTIONE DEGLI INCIDENTI DI SICUREZZA 14
9. FASI DELLA PROCEDURA DI GESTIONE DEGLI INCIDENTI DI SICUREZZA 15
9.1. PREPARAZIONE 15
9.2. IDENTIFICAZIONE E ANALISI DELL'INCIDENTE 16
9.3. VALUTAZIONE DELL'IMPATTO DELL'INCIDENTE 16
9.4. COMUNICAZIONE DEGLI INCIDENTI 19
9.4.1. COMUNICAZIONE INTERNA 20
9.4.2. COMUNICAZIONE ESTERNA 20
9.4.3. COMUNICAZIONE FINALE 20
9.4.4. COMUNICAZIONE DATA BREACH 21
9.4.5. COMUNICAZIONE INCIDENTE DI SICUREZZA AL CSIRT 21
9.4.6. COMUNICAZIONE DI INFORMAZIONI PERTINENTI AL CSIRT 22
9.5. ATTIVAZIONE DELLA PROCEDURA E MONITORAGGIO DELLE ATTIVITÀ 23
9.5.1. INCIDENTE DI LIVELLO L3 O L4 (GRAVITÀ ALTA O CRITICA) 23
9.5.2. INCIDENTE DI LIVELLO L1 O L2 (GRAVITÀ BASSA O MEDIA) 23
9.6. CONTENIMENTO, RIMOZIONE E RIPRISTINO 24
9.6.1. CONTENIMENTO A BREVE TERMINE 24
9.6.2. CONTENIMENTO A LUNGO TERMINE 25
9.6.3. RIMOZIONE 25
9.6.4. RIPRISTINO 26
9.7. ATTIVITÀ POST-INCIDENTE 26
9.8. FORMAZIONE E SENSIBILIZZAZIONE 29
9.9. REVISIONE E AGGIORNAMENTO DELLA PROCEDURA 29
9.9.1. INFORMAZIONI DOCUMENTATE 29
ALLEGATO 1: ISTRUZIONI PER GLI UTENTI PER LA SEGNALAZIONE DELL'INCIDENTE 31
ALLEGATO 2: TEMPLATE MODULO RAPPORTO INCIDENTE DI SICUREZZA 32
ALLEGATO 3: DATABASE INCIDENTI SICUREZZA 34
ALLEGATO 4: REGOLE PER L'IDENTIFICAZIONE, LA RACCOLTA E LA CONSERVAZIONE DELLE PROVE 35

1. INTRODUZIONE

Il Comune di Parma adotta un proprio modello organizzativo e di governo per la gestione della sicurezza delle informazioni e della cybersicurezza, nell'ambito del quale sono definiti ruoli, responsabilità, autorità e funzioni di indirizzo, governo, supervisione e controllo.

Per l'attuazione operativa di tale modello, il Comune si avvale del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) adottato da IT.CITY S.p.A., società in house dell'Ente, nonché delle relative politiche, procedure, metodologie e misure di sicurezza, per quanto applicabili ai servizi affidati e al perimetro comunale.

Restano in capo al Comune di Parma la governance complessiva della sicurezza, l'indirizzo strategico, il governo e l'accettazione del rischio, l'approvazione delle misure e dei piani di propria competenza, la supervisione e la vigilanza sulla loro attuazione, in conformità al Decreto Legislativo 4 settembre 2024, n. 138 e alle altre disposizioni applicabili in materia di cybersicurezza.

La presente procedura rappresenta il riferimento per il Comune di Parma per la regolamentazione della gestione degli incidenti di sicurezza delle informazioni che possono occorrere ai servizi ed ai dati gestiti e ha l'obiettivo di definire un processo strutturato per l'identificazione, la classificazione, la gestione, la risoluzione e la rendicontazione degli incidenti di sicurezza informatica che possono compromettere la riservatezza, l'integrità e la disponibilità dei dati, dei sistemi e dei servizi informatici dell'Ente.
Essa mira a garantire:

- l'efficace gestione degli incidenti di sicurezza;
- la riduzione dell'impatto degli incidenti sulle operazioni aziendali;
- la protezione dei dati personali e sensibili trattati, del Comune di Parma;
- il rispetto degli obblighi normativi in materia di cybersecurity;
- il miglioramento continuo delle misure di sicurezza.

La procedura di gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati gestiti; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità di intervento, un continuo miglioramento delle capacità di risposta del Comune di Parma.

La procedura attua gli artt. 23, 24, 25 e 26 del D.Lgs. 4 settembre 2024, n. 138, con particolare riferimento alla governance, alla gestione degli incidenti, alla qualificazione degli incidenti significativi, alle notifiche obbligatorie e volontarie al CSIRT Italia e alle comunicazioni ai destinatari dei servizi.
Inoltre, con specifico riferimento all'obbligo di cui all'art. 33 del GDPR n. 679/2016, il presente documento individua quali siano le violazioni che ricadono nell'ambito della suddetta normativa, i casi in cui l'Ente debba notificare i data breach all'Autorità Garante e agli interessati e le misure atte a trattare il rischio e la documentazione da produrre.
L'art. 32 del Regolamento dispone che devono essere approntate misure tecniche e organizzative atte a garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente un incidente di sicurezza, come una violazione di dati, è espressione dell'adeguatezza delle misure implementate dall'Ente.

Tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali. L'obbligo di cui agli artt. 33 e 34 del Regolamento trova applicazione nei soli casi in cui la violazione riguardi dati personali, come definiti dall'art. 4 n. 1).
La procedura è gestita secondo le clausole 4-10 della ISO/IEC 27001:2022. Contesto, criteri e priorità derivano dalla valutazione del rischio e dalla Business Impact Analysis; i controlli applicabili sono tracciati nella valutazione del rischio; incidenti, lezioni apprese, non conformità e rischi residui aggiornano Piano di Trattamento, Piano di Adeguamento, Piano di Formazione e obiettivi di miglioramento.

2. SCOPO E CAMPO DI APPLICAZIONE

Lo scopo di questo documento è quello di definire cos'è un incidente di sicurezza, quali sono i ruoli e le responsabilità nell'ambito della gestione degli incidenti di sicurezza e descrivere la procedura di gestione e le fasi che la caratterizzano. La procedura è integrata dall'Allegato 4, che disciplina in modo specifico le regole per l'identificazione, la raccolta e la conservazione delle prove relative agli incidenti di sicurezza delle informazioni.

Vi sono comportamenti, attività e regolamenti che ogni organizzazione deve necessariamente attivare per cercare di prevenire gli incidenti di sicurezza, riducendo il livello di rischio e l'esposizione a possibili attacchi informatici. Tali contromisure, che possono essere di natura sia tecnologica che organizzativa, devono essere descritte e adottate dal Comune di Parma per mettere in sicurezza i sistemi ICT.

La presente procedura si applica:
- A tutti i sistemi informativi, le reti, le infrastrutture, le applicazioni, i dati e i servizi digitali gestiti internamente o da fornitori terzi per conto dell'organizzazione;
- A tutto il personale interno, ai collaboratori esterni e ai fornitori che operano sui sistemi o trattano dati per conto dell'organizzazione;

A ogni incidente, potenziale o confermato, che possa determinare un rischio per la sicurezza informatica o la continuità operativa.

Il Dirigente della Transizione Digitale è responsabile della redazione, revisione e aggiornamento della presente procedura.
Destinatario del piano sono i membri del gruppo di Coordinamento e di Gestione degli Incidenti (descritto nel paragrafo dedicato ai ruoli), il personale del Settore ITC e tutto il personale dell'Ente coinvolto a vario titolo nella risposta agli incidenti di sicurezza.

3. RIFERIMENTI

- Linee Guida AGID per la gestione degli incidenti di sicurezza
- Direttiva (UE) 2022/2555 (NIS2)
- D.Lgs. 4 settembre 2024, n. 138, in particolare artt. 23-26, 30-32 e 38, nelle parti applicabili.
- Determinazione ACN n. 379907/2025, che integra e sostituisce la Determinazione n. 164179/2025, e relativi Allegati 1-4 concernenti misure di sicurezza e incidenti significativi per soggetti importanti ed essenziali.
- Linee Guida NIS – Specifiche di base per la definizione del processo di gestione degli

incidenti di sicurezza informatica e provvedimenti ACN vigenti su Portale ACN, Servizi NIS e Referente CSIRT.
- ISO/IEC 27001:2022 e ISO/IEC 27002:2022, in particolare A.5.7, A.5.24-A.5.28, A.5.30, A.7.4, A.8.9, A.8.12, A.8.15 e A.8.16.
- Framework documentale specifico Comune di Parma
- Framework documentale IT.CITY S.P.A. Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
- ISO/IEC 27035:2023
- NIST SP 800-61r3 – Computer Security Incident Handling Guide
- Regolamento Generale sulla Protezione dei Dati GDPR EU 2016/679, D.lgs. n. 196 del 30 giugno 2003 così come modificato dal D.lgs. 101 del 10 agosto 2018, Provvedimenti e Autorizzazioni Generali dell'Autorità Garante e qualsiasi altra norma applicabile avente ad oggetto il trattamento di dati personali
- Contratto di Servizio per la gestione del sistema informativo tra Comune di Parma ed IT City SPA.
- Regolamento sull'Ordinamento degli Uffici e dei Servizi
- Regolamento per l'utilizzo dei sistemi informativi e delle risorse informatiche, telematiche e telefoniche dell'amministrazione.

4. DEFINIZIONI

- Evento di sicurezza: qualunque occorrenza osservabile che abbia rilevanza per la sicurezza delle informazioni o dei sistemi informativi.
- Incidente di sicurezza: evento confermato che compromette la riservatezza, l'integrità o la disponibilità di dati, sistemi o servizi informatici.
- Gravità dell'incidente: livello di severità assegnato a un incidente di sicurezza sulla base di impatto, durata, diffusione e criticità dei servizi coinvolti, utilizzato per determinare priorità di gestione, comunicazione e notifica.
- Knowledge base degli incidenti: archivio strutturato, ad accesso controllato, contenente informazioni anonimizzate sugli incidenti di sicurezza, utilizzato per attività di analisi, formazione e miglioramento continuo.
- Continuità operativa: capacità dell'organizzazione di mantenere o ripristinare i servizi essenziali entro tempi accettabili a seguito di un incidente di sicurezza, in coordinamento con i piani di Business Continuity e Disaster Recovery.
- Ripristino: fase della gestione dell'incidente finalizzata al ritorno dei sistemi e dei servizi a condizioni operative sicure e controllate.
- CSIRT Italia: il Gruppo di intervento nazionale per la sicurezza informatica operante presso ACN, destinatario delle notifiche obbligatorie e volontarie previste dagli artt. 25 e 26 del D.Lgs. 138/2024. Il gruppo interno di risposta è denominato "Gruppo di Coordinamento e di Gestione degli Incidenti" per evitare ambiguità.
- DPO (Data Protection Officer): figura responsabile della conformità al Regolamento (UE) 2016/679 in materia di protezione dei dati personali.
- Punto di Contatto NIS: persona fisica designata dal Comune per curare gli adempimenti e l'interlocuzione istituzionale con ACN tramite il Portale ACN, inclusa la designazione del Referente CSIRT e dei relativi sostituti, secondo i provvedimenti vigenti.
- Sostituto del Punto di Contatto NIS: persona fisica distinta che assicura continuità

nello svolgimento degli adempimenti e può operare nei limiti delle abilitazioni e delle disposizioni ACN vigenti.

- Referente CSIRT: persona fisica, interna o esterna e dotata di adeguate competenze tecniche, designata dal Punto di Contatto tramite il Portale ACN per interfacciarsi con CSIRT Italia ed effettuare le notifiche degli artt. 25 e 26 per conto del Comune; sono individuati uno o più sostituti per garantire continuità e reperibilità.
- Incidente significativo (NIS2): incidente che ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il Comune, oppure che ha avuto o può avere ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli. La valutazione considera anche la tipologia prevista dall'Allegato 3 o 4 della Determinazione ACN vigente, in funzione della qualificazione del Comune che è soggetto Importante.
- Significatività dell'incidente: valutazione distinta dal livello interno L1-L4, effettuata e rivalutata senza ritardo sulla base dell'art. 25 del D.Lgs. 138/2024, delle specifiche ACN applicabili, della criticità dei servizi, della durata, dell'estensione, degli utenti e soggetti coinvolti, degli impatti economici, sociali e transfrontalieri e delle evidenze disponibili.
- Notifica NIS2: comunicazione formale trasmessa al CSIRT Italia dal Referente CSIRT o da un sostituto abilitato, mediante il servizio dedicato del Portale ACN, nei termini e con i contenuti di cui all'art. 25 del D.Lgs. 138/2024. Le ricevute, i protocolli e gli allegati sono conservati nel fascicolo dell'incidente.
- Pre-notifica NIS2: comunicazione trasmessa senza ingiustificato ritardo e comunque entro 24 ore da quando il Comune è venuto a conoscenza dell'incidente significativo; ove possibile indica se l'evento può derivare da atti illegittimi o malevoli o avere impatto transfrontaliero.
- Prova / Evidenza: informazione, dato o oggetto, in formato digitale o fisico, raccolto e conservato secondo le regole definite nell'Allegato 4, idoneo a supportare attività di analisi, investigazione o azione legale.
- Catena di custodia (Chain of Custody) Processo documentato che garantisce la tracciabilità completa di una prova/evidenza, dalla sua acquisizione fino alla distruzione, assicurando l'integrità, l'autenticità e l'utilizzabilità della stessa in ambito investigativo, disciplinare o giudiziario.
- Evidenza digitale forense: Prova digitale acquisita mediante tecniche idonee a preservarne l'integrità e il valore probatorio, raccolta e conservata secondo procedure tali da consentirne l'utilizzo in procedimenti investigativi o giudiziari.
- Registro delle evidenze: Documento o sistema informativo utilizzato per registrare, gestire e monitorare le evidenze raccolte durante la gestione di un incidente di sicurezza, comprensivo delle informazioni relative alla catena di custodia, ai soggetti autorizzati e ai tempi di conservazione.
- Momento di conoscenza dell'incidente: data e ora in cui il Comune dispone di elementi sufficienti per riconoscere l'esistenza dell'incidente. Il timestamp, la fonte e il responsabile della valutazione sono registrati immediatamente e costituiscono il riferimento per il calcolo dei termini NIS2 e, separatamente, GDPR.
- Relazione finale NIS2: relazione trasmessa entro un mese dalla notifica delle 72 ore e contenente descrizione dettagliata, gravità e impatto, minaccia o root cause, misure

di attenuazione adottate e in corso ed eventuale impatto transfrontaliero. Se l'incidente è ancora in corso, sono trasmesse relazioni mensili sui progressi e una relazione finale entro un mese dalla conclusione della gestione.

- Notifica NIS2 entro 72 ore: comunicazione che aggiorna la pre-notifica e fornisce una prima valutazione della gravità e dell'impatto e, ove disponibili, gli indicatori di compromissione.
- Relazione intermedia NIS2: aggiornamento sulla situazione trasmesso su richiesta del CSIRT Italia.
- Accountability (responsabilizzazione): Principio secondo cui il Comune di Parma deve essere in grado di dimostrare, attraverso evidenze documentate, l'adozione e l'efficacia delle misure tecniche e organizzative previste per la gestione degli incidenti di sicurezza.
- Decisione di attivazione forense: Valutazione formale effettuata dal gruppo di Coordinamento e di Gestione degli Incidenti di sicurezza o dal Referente CSIRT, finalizzata a stabilire se un incidente richiede la raccolta delle evidenze con modalità forensi, in considerazione di possibili sviluppi legali o giudiziari.
- Copia forense bit-stream (bit-by-bit copy): Copia integrale e fedele di un supporto di memorizzazione digitale, effettuata a livello di singolo bit, comprensiva di dati attivi, dati cancellati, spazio non allocato e metadati, realizzata con strumenti idonei a preservare l'integrità e il valore probatorio dell'evidenza.
- Hash crittografico (checksum di integrità): Valore univoco generato mediante funzione crittografica (es. SHA-256) utilizzato per verificare l'integrità di una prova digitale e dimostrare che non ha subito alterazioni nel tempo.
- Strumenti forensi: Software o hardware specializzati utilizzati per l'acquisizione, l'analisi e la conservazione di evidenze digitali, progettati per garantire l'integrità dei dati e la tracciabilità delle operazioni effettuate.
- Ambiente di conservazione sicuro delle evidenze: Ambiente fisico o logico protetto, segregato e controllato, destinato alla conservazione delle evidenze raccolte durante la gestione degli incidenti di sicurezza, con accessi limitati, tracciati e autorizzati.
- Operazioni distruttive: Attività tecniche che possono alterare, sovrascrivere o cancellare dati o configurazioni di un sistema informativo, quali aggiornamenti, reinstallazioni, ripristini o pulizie dei log.
- Valore probatorio: Capacità di una prova o evidenza di essere utilizzata in modo valido e attendibile in procedimenti investigativi, disciplinari o giudiziari, grazie al rispetto delle regole di integrità, tracciabilità e conservazione.
- Acquisizione forense: Processo strutturato di raccolta di evidenze digitali effettuato secondo tecniche e procedure idonee a preservarne l'integrità e il valore probatorio, inclusa la generazione e la verifica di hash crittografici.
- Minimizzazione delle evidenze: Principio secondo cui devono essere raccolte esclusivamente le evidenze strettamente necessarie alla gestione dell'incidente, evitando acquisizioni eccessive o non pertinenti.

5. INCIDENTE DI SICUREZZA

Un "incidente di sicurezza" è un evento che ha causato o può potenzialmente causare danni agli asset, causare la violazione o la minaccia imminente di violazione di una politica di sicurezza informatica, correlato ad una violazione di dati o informazioni.

Un incidente può essere un evento che colpisce negativamente l'elaborazione dei sistemi informatici.

Questi alcuni esempi:
- Perdita della riservatezza di dati o delle informazioni
- Invio di informazioni a destinatari che non sono autorizzati alla loro consultazione
- Perdita di integrità delle informazioni
- Riduzione o totale inibizione del funzionamento del sistema (Denial of service)
- Accessi non autorizzati a dati, informazioni o sistemi
- Uso improprio dei sistemi o delle informazioni
- Modifica di informazioni, dati, configurazioni hardware o software senza le procedure corrette o i consensi necessari
- Danneggiamento e furto dei sistemi
- Uso non autorizzato di un sistema per il trattamento o la conservazione di dati
- Attacchi virus o malware

Di seguito alcuni esempi di azioni atte a causare un incidente di sicurezza:
- un utente malintenzionato esegue operazioni al fine di inviare un numero elevato di richieste di connessione ad un server web, provocando l'arresto anomalo del servizio;
- gli utenti sono indotti ad aprire un file allegato alla mail che in realtà è un malware; l'esecuzione del tool che comporta l'infezione del dispositivo stabilendo connessioni con un host esterno;
- un utente malintenzionato ottiene dati sensibili e minaccia l'organizzazione di diffonderli se non viene pagato un riscatto in denaro.

Alcuni eventi che interessano il personale interno che si configurano come incidenti che riguardano la sicurezza delle informazioni includono:
- Perdita del badge personale
- Perdita della corrispondenza sia cartacea che elettronica
- Stampe dimenticate sulle quali vi erano informazioni almeno confidenziali
- Perdita dei supporti di memorizzazione
- Perdita delle password
- Perdita dei cellulari o dei pc portatili
- Furto, perdita o manomissione di documenti cartacei

6. DATA BREACH AI SENSI DEL GDPR

Il Regolamento Generale sulla Protezione dei Dati definisce la violazione dei dati personali come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".
Le violazioni declinate dalla norma sono sintetizzabili come:
- "Violazione della riservatezza", che si ha in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali
- "Violazione dell'integrità", che si ha in caso di alterazione non autorizzata o accidentale dei dati personali
- "Violazione della disponibilità", che si ha in caso di perdita o distruzioni di dati personali o di impossibilità di accesso ai dati personali da parte di soggetti autorizzati.

Va sottolineato che una violazione può riguardare contemporaneamente la riservatezza,

l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione di queste.

7. RUOLI E RESPONSABILITÀ

La criticità del processo di gestione degli incidenti di sicurezza informatica e del data breach deve essere opportunamente affrontata da una struttura operativa competente, in possesso di adeguata formazione ed in grado di prendere rapidamente le decisioni imposte dalla delicatezza del compito assegnato.
Per tale motivo l'Ente istituisce il Gruppo di Coordinamento e di Gestione degli Incidenti con le seguenti competenze:
Gli Organi di Amministrazione e Direttivi approvano le modalità di implementazione della presente procedura, ne sovrintendono l'efficacia e sono informati periodicamente e, per gli incidenti significativi o critici, tempestivamente. Il RTD assicura il coordinamento e l'escalation; il Referente CSIRT cura le notifiche a CSIRT Italia; il Punto di Contatto presidia gli adempimenti istituzionali sul Portale ACN; il DPO gestisce le valutazioni e gli adempimenti GDPR, che restano autonomi e paralleli.

- rappresentare il punto di coordinamento univoco sia in fase di preparazione che in fase di gestione e risposta agli incidenti;
- gestire tutte le fasi e tutte le attività inerenti l'analisi e la gestione di un incidente di sicurezza, ivi comprese quelle relative alla sua notifica e documentazione;
- garantire la disponibilità delle liste di contatti (es.: personale dipendente, collaboratori, fornitori), necessarie per la gestione di un incidente di sicurezza;
- predisporre adeguati test e simulazioni periodici di incidenti di sicurezza;
- garantire che il processo di gestione incidenti sia sempre adeguato alle esigenze dell'Ente, facendo sì che sia aggiornato a seguito di cambiamenti tecnologici, infrastrutturali e organizzativi e a fronte di incidenti di sicurezza che mettano in evidenza aspetti di miglioramento nella procedura stessa.

Il gruppo di Coordinamento e di Gestione degli Incidenti deve essere composto dalle seguenti figure di riferimento:

- Dirigente Responsabile per la Transizione Digitale / CIO
- Direttore Operativo IT.CITY S.p.A.
- Referente CSIRT (Responsabile tecnico IT.CITY S.p.A.)
- Responsabile della Comunicazione Istituzionale
- Referente cyber Transizione Digitale (Punto di contatto NIS o suo sostituto)
- Referente del team RTD dell'Ente che possiede competenze utili alla risoluzione dell'incidente;
- Referente del Gruppo Privacy che può fornire informazioni utili alla risoluzione dell'incidente informatico.

In funzione della tipologia di evento, il gruppo di Coordinamento può essere esteso a:

- Direttore Generale / Segretario Generale
- Sindaco o Assessore delegato
- Data Protection Officer (DPO)
- Responsabile Protezione Civile
- Responsabili dei servizi comunali impattati
- Fornitori critici (es. Lepida S.c.p.A.)

La procedura di gestione degli incidenti di sicurezza deve essere anche supportata da una struttura operativa che:

- rappresenti il punto di riferimento univoco a cui il personale dell'organizzazione deve rivolgersi per segnalare un potenziale incidente oppure un comportamento sospetto;
- gestisca tutte le attività inerenti all'analisi e alla risoluzione di un incidente di sicurezza, ivi comprese quelle relative alla sua notifica e documentazione;
- garantisca la disponibilità delle liste di contatti (es.: personale dipendente, collaboratori, fornitori), necessarie per la gestione di un incidente di sicurezza;
- garantisca che il processo di gestione incidenti sia sempre adeguato alle esigenze del Comune di Parma e sia sempre aggiornato;
- rappresenti il punto di riferimento dell'organizzazione come interlocutore diretto con l'agenzia nazionale per la cybersicurezza (ACN);
- gestisca la registrazione e l'aggiornamento dei dati sulla piattaforma messa a disposizione da ACN.

Nel corso del processo di gestione di un incidente di sicurezza informatico e, eventualmente, di un data breach, il gruppo potrà essere coadiuvato di volta in volta dal personale della struttura i cui dati sono stati oggetto di data breach e da tutti coloro che il gruppo riterrà necessario coinvolgere a seconda della tipologia di incidente e della tipologia di dati coinvolti.

Nelle attività del gruppo per la Gestione della Sicurezza Informatica deve essere coinvolto il Data Protection Officer (DPO), il quale esercita le proprie funzioni di monitoraggio della conformità in caso di data breach, fornendo il proprio parere in ordine alla necessità di effettuare la notifica e, quindi, sulle valutazioni precedentemente descritte.

Il Gruppo individua quale Coordinatore il Responsabile per la Transizione Digitale, che attiva e coordina il gruppo, assicura la classificazione e l'escalation, autorizza le misure urgenti nei limiti delle competenze e coinvolge il DPO per i dati personali. Quando ricorrono o possono ricorrere i criteri dell'incidente significativo, il Coordinatore informa immediatamente il Referente CSIRT e i suoi sostituti, affinché la pre-notifica, la notifica e le relazioni siano trasmesse al CSIRT Italia nei termini. Il Punto di Contatto NIS è informato e assicura il raccordo istituzionale con ACN; le notifiche GDPR sono curate dal Titolare con il supporto del DPO secondo il processo applicabile.
Il Coordinatore deve inoltre coinvolgere, a seconda della gravità dell'incidente, il Sindaco e il Direttore Generale per gli aspetti di comunicazione interna ed esterna e, nel caso in cui emergano responsabilità da parte di personale interno, occorre coinvolgere la struttura che si occupa della gestione del personale.
Nel caso in cui le attività di analisi dell'incidente di sicurezza evidenzino particolari difficoltà, oppure impatti che si estendono al di fuori del perimetro dell'Ente, il coordinatore deve valutare l'opportunità o la necessità, di coinvolgere le strutture di riferimento regionali e nazionali. Inoltre, il Coordinatore deve valutare se coinvolgere i propri fornitori nelle attività di analisi e gestione dell'incidente, se l'incidente presenta risvolti dal punto di vista penale il Coordinatore deve coinvolgere le autorità di pubblica sicurezza.
I contratti con fornitori e subfornitori rilevanti prevedono canali di escalation, reperibilità, cooperazione, disponibilità dei log e delle evidenze, obbligo di notifica a cascata senza ritardo e tempi compatibili con gli obblighi del Comune.

Di seguito la tabella per ruoli e responsabilità definiti

RUOLO	RESPONSABILITA'
Dirigente Responsabile per la Transizione Digitale/CIO/CISO	Coordina il Gruppo, assicura classificazione L1-L4 e valutazione della significatività NIS2, autorizza le azioni urgenti nei limiti delle competenze, informa gli Organi di Amministrazione e Direttivi e verifica che rischi, Piano di Tattamento/Adeguamento e lezioni apprese siano aggiornati. Oltre a coordinare il "Gruppo di Coordinamento e di Gestione degli Incidenti" è responsabile: - della corretta tenuta dei security incident report e di tutte le evidenze raccolte durante la gestione degli incidenti; - dell'individuazione della modalità di risoluzione delle vulnerabilità segnalate da ACN in seguito ad incidenti di sicurezza o ad audit, sulla base di quanto previsto dalla Legge 90/2024 (art. 2 comma1); Sovrintendere l'intero processo di gestione degli incidenti, coordinare le attività di analisi, contenimento e notifica, autorizzare il report conclusivo e proporre azioni correttive.
Gruppo di coordinamento e di gestione degli incidenti di sicurezza	E' responsabile di garantire che il processo di gestione incidenti sia sempre adeguato alle esigenze dell'Ente, provvedendo che sia sempre aggiornato: Assume la gestione operativa dell'incidente, e potrà essere coadiuvato di volta in volta da specialisti IT, personale della Struttura dell'Ente i cui dati sono stati eventualmente oggetto di violazione, da tutti coloro che riterrà necessario coinvolgere a seconda della tipologia di incidente e della tipologia di dati coinvolti. È inoltre responsabile della preparazione e gestione operativa delle simulazioni di incidenti.
Team IT	Deve identificare e analizzare gli incidenti, attuare le misure di contenimento e mitigazione, raccogliere evidenze, comunicare con i referenti interni ed esterni.
DPO	Deve valutare l'impatto dell'incidente sui dati personali, curare le eventuali notifiche al Garante per la protezione dei dati personali e agli interessati.
Punto di Contatto	Cura gli adempimenti e l'interlocuzione istituzionale con ACN tramite il Portale ACN, mantiene aggiornati i dati e designa il Referente CSIRT e i sostituti secondo i provvedimenti vigenti. Non sostituisce il Referente CSIRT nella gestione tecnica e nelle notifiche, salvo specifica abilitazione prevista da ACN.
Sostituto Punto di Contatto	Assicura continuità al Punto di Contatto NIS e opera nei limiti delle deleghe e delle abilitazioni attribuite; mantiene aggiornati recapiti e disponibilità.
Referente CSIRT	Interagisce direttamente con CSIRT Italia ed effettua, con i sostituti abilitati, pre-notifica, notifica, relazioni intermedie, relazione finale e notifiche volontarie tramite il Portale ACN; conserva ricevute e protocolli e assicura reperibilità, competenza tecnica e qualità delle informazioni trasmesse.

RUOLO	RESPONSABILITA'
Alta Direzione (Sindaco/Direttore Generale/Segretario Generale)	Approva la procedura e le comunicazioni esterne rilevanti, sovrintende all'implementazione, riceve reporting periodico e tempestivo, autorizza le decisioni strategiche, l'eventuale attivazione della crisi e le risorse necessarie, nel rispetto delle competenze istituzionali.
Personale Dipendenti	Segnalare tempestivamente eventi sospetti o anomalie secondo quanto previsto dalle policy

8. PROCEDURA DI GESTIONE DEGLI INCIDENTI DI SICUREZZA

La procedura di gestione degli incidenti informatici di sicurezza richiede che:

- sia definita la struttura tecnica di supporto nella gestione degli incidenti e dei necessari interventi di formazione per le risorse potenzialmente coinvolte nella gestione degli incidenti;
- siano predisposti gli strumenti hardware e software necessari;
- siano definite e distribuite le apposite procedure relative alle modalità di comunicazione dell'accaduto verso l'esterno.

La procedura di gestione degli incidenti di sicurezza, che deve essere sviluppata, documentata e tenuta aggiornata, ha i seguenti obiettivi:

- rispondere alla normativa applicabile;
- preparare il personale;
- identificare un incidente in corso;
- minimizzare i danni relativi all'incidente ed impedirne la propagazione;
- gestire correttamente il processo di ripristino dei sistemi e delle applicazioni;
- acquisire nel modo appropriato le eventuali evidenze digitali di reato;
- riconoscere gli errori commessi, assumerne le responsabilità e formulare proposte volte a migliorare la procedura stessa.

La decisione su quali soluzioni adottare è demandata al gruppo di gestione sicurezza con l'eventuale supporto delle figure ritenute necessarie tenendo conto della complessità e variabilità dell'argomento trattato.

Oltre ai requisiti di riservatezza ed integrità, occorre considerare anche le esigenze di disponibilità dei dati e dell'infrastruttura ICT preposta all'erogazione dei servizi informatici. Nel caso si verifichi un incidente di sicurezza che possa pregiudicare per un periodo sufficientemente lungo la disponibilità delle informazioni occorre fare riferimento a disposizioni contenute nel piano di continuità operativa predisposto dall'Ente e in concerto con la società partecipata IT.CITY S.p.A. con una chiara definizione delle strutture e delle responsabilità della gestione delle emergenze che dovranno operare in stretto coordinamento con il gruppo gestione sicurezza

Qualora, a seguito di un incidente relativo alla sicurezza delle informazioni, risulti necessario per l'Ente intraprendere un'azione legale (civile o penale) contro una persona fisica o giuridica, oppure nel caso in cui ci siano le premesse affinché l'Ente possa essere oggetto di azione legale (civile o penale), le evidenze oggettive devono essere raccolte e conservate e presentate al fine di conformarsi ai requisiti di legge applicabili nelle sedi giurisdizionali competenti. Tutta la fase di raccolta delle evidenze deve essere fatta in modo che le evidenze

siano utilizzabili in un processo giuridico. La raccolta delle evidenze può avvenire anche qualora si voglia semplicemente procedere con indagini più approfondite, non necessariamente legate ad un proseguo forense.

La documentazione relativa agli incidenti, incluse evidenze, valutazioni e notifiche, è trattata secondo criteri di minimizzazione, integrità, riservatezza e necessità. I tempi di conservazione sono definiti nel piano di conservazione documentale dell'Ente, (che è in fase di aggiornamento), tenendo conto degli obblighi normativi, delle prescrizioni ACN, delle finalità di audit, dell'accertamento di responsabilità e di eventuali contenziosi o legal hold. Alla scadenza, i dati personali e le evidenze sono cancellati, anonimizzati o ulteriormente conservati solo in presenza di una base giuridica documentata.

Tutti i dipendenti e collaboratori dell'Ente che accedono alle risorse del Sistema Informatico del Comune di Parma sono tenuti ad osservare i principi contenuti nel presente documento ed a segnalare in modo tempestivo la presenza di condizioni che possano indurre a valutare delle anomalie riconducibili ad attacchi informatici oppure a comportamenti scorretti.
Eventuali amministratori di sistema, che a causa del loro comportamento gravemente negligente o in palese contrasto con le politiche di sicurezza dell'Ente, fossero causa diretta o indiretta di incidente di sicurezza, potranno essere soggetti ad un accertamento di eventuali responsabilità e violazione delle politiche di sicurezza ICT dell'Ente.

9. FASI DELLA PROCEDURA DI GESTIONE DEGLI INCIDENTI DI SICUREZZA

9.1. PREPARAZIONE

Si tratta di attività necessarie per consentire una adeguata gestione degli incidenti informatici di sicurezza che devono essere eseguite rigorosamente.
La fase di preparazione comprende tutte le attività da svolgere prima che un incidente si verifichi, con l'obiettivo di garantire che l'Ente sia organizzativamente e operativamente pronto a gestirlo
Si tratta ad esempio di:

- definizione della struttura tecnica di supporto nella gestione degli incidenti e dei necessari interventi di formazione per le risorse potenzialmente coinvolte nella gestione degli incidenti;
- predisposizione degli strumenti hardware e software necessari;
- definire e distribuire le apposite procedure relative alle modalità di comunicazione verso l'esterno dell'accaduto.
- mantenere accessi, credenziali, ruoli e sostituti per il Portale ACN, modelli di pre-notifica/notifica/relazione, contatti protetti e canali alternativi da utilizzare esclusivamente secondo le indicazioni ACN in caso di indisponibilità del Portale;
- assicurare fonti di rilevamento e registrazione coerenti con i controlli applicabili, tra cui threat intelligence (A.5.7), alert dei servizi cloud (A.5.23), monitoraggio fisico (A.7.4), DLP (A.8.12), logging e monitoraggio (A.8.15-A.8.16), web filtering (A.8.23), gestione delle configurazioni (A.8.9) e segnalazioni dei fornitori;
- eseguire almeno annualmente esercitazioni integrate con Piano di Gestione delle Crisi, Business Continuity e Disaster Recovery, includendo decisione sulla significatività, indisponibilità dei canali ordinari, notifiche al CSIRT Italia e comunicazioni ai destinatari.

9.2. IDENTIFICAZIONE E ANALISI DELL'INCIDENTE

Si tratta di attività che mira a valutare se un evento riscontrato sia effettivamente riconducibile ad un incidente di sicurezza oppure si tratti di un cosiddetto falso positivo. Le operazioni di identificazione (Detection and Analysis) devono permettere di verificare, per ogni caso di evento anomalo o sintomo di un incidente, se si è in presenza di un incidente reale di sicurezza.
La segnalazione di incidente di sicurezza può arrivare:

- direttamente da parte di un utente, il quale può per esempio rilevare situazioni di alterazione di un sito web dell'Ente, di accesso non autorizzato a dati, di indisponibilità di una risorsa ICT per un tempo prolungato etc. Le segnalazioni degli utenti devono pervenire ad una struttura opportunamente identificata e preparata per condurre una prima analisi prima di coinvolgere il gruppo Gestione Sicurezza ICT.
- direttamente tramite strumenti che in automatico informano l'ICT sulla situazione di funzionamento anomalo dei sistemi esempio sistemi di monitoraggio (SIEM, IDS/IPS, antivirus, firewall)
- comunicazioni da fornitori o da soggetti esterni. I fornitori devono segnalare senza ritardo gli eventi che possono incidere sui servizi del Comune e fornire le informazioni disponibili, inclusi timeline, impatto, indicatori di compromissione, azioni di contenimento, subfornitori coinvolti e modalità di accesso alle evidenze, secondo le clausole contrattuali vigenti.
- allerta da parte del CSIRT nazionale, CERT, Forze dell'Ordine o altri enti istituzionali.

Tutti gli eventi sospetti devono essere registrati in un sistema di ticketing o registro eventi.
La registrazione iniziale deve riportare almeno data e ora della segnalazione, data e ora del momento di conoscenza, fonte, sistemi e servizi coinvolti, responsabile della prima valutazione, livello L1-L4 provvisorio, possibile rilevanza NIS2/GDPR, fornitori coinvolti ed evidenze preservate. La classificazione è rivalutata durante l'intero ciclo di gestione e ogni variazione è tracciata.
Nel caso in cui venga rilevato un riscontro positivo durante l'analisi di tali eventi viene aperto un incidente di sicurezza che segue la procedura di gestione. Durante la fase di analisi devono essere identificate e preservate le potenziali evidenze dell'incidente, secondo quanto previsto dall'Allegato 4.
Se l'indagine conferma una violazione di dati personali, il Coordinatore coinvolge immediatamente il DPO e il Titolare documenta la valutazione del rischio per i diritti e le libertà degli interessati, determinando gli eventuali adempimenti verso il Garante e gli interessati ai sensi degli artt. 33 e 34 GDPR. La qualificazione e la notifica NIS2 sono valutate separatamente secondo i criteri dell'art. 25 del D.Lgs. 138/2024; un medesimo incidente può richiedere entrambi i flussi.

Qualora l'incidente comporti un'indisponibilità dei servizi critici superiore ai livelli minimi di servizio definiti dal Comune di Parma, viene attivato il **Piano di Business Continuity** e, se necessario, il **Piano di Disaster Recovery**

9.3. VALUTAZIONE DELL'IMPATTO DELL'INCIDENTE

L'analisi degli eventi può portare all'individuazione dei possibili reali incidenti di sicurezza, che si possono classificare in diverse tipologie come segue:

TIPOLOGIA INCIDENTE	DESCRIZIONE
Accesso non autorizzato	Accesso (sia logico che fisico) a reti, sistemi, applicazioni, dati o altre risorse tecnologiche di proprietà di IT.CITY da parte di personale non autorizzato.
Denial of Service	Attacco informatico alla disponibilità di una rete o sistema. Qualora abbia successo, comporta la difficoltà all'accesso o la totale indisponibilità di determinati sistemi e/o servizi.
Codice malevolo	Un virus, worm, trojan, spyware, o qualsiasi altro codice malevolo che infetti un sistema.
Uso Inappropriato	Violazione delle politiche di sicurezza e delle disposizioni su corretto utilizzo.
Data leakage	Diffusione di informazioni riservate a seguito di un attacco informatico riuscito.
Alterazione delle informazioni	Modifica del contenuto di dati riservati a seguito di un attacco informatico riuscito.
Phishing	Truffa effettuata su Internet, che sfrutta tecniche di ingegneria sociale, attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso.
Furto/smarrimento totale o parziale di apparecchiature che contengono dati sensibili	Il furto o smarrimento di singoli dispositivi di memorizzazione (hard disk, memorie di massa rimovibili ecc) oppure dei computer/server che li ospitano. Una violazione dei dati personali sensibili contenuti configura una condizione di data breach che richiede, ai sensi del GDPR, l'attivazione delle specifiche procedure di notifica verso l'autorità Garante e gli utenti coinvolti
Multiplo	Incidente di sicurezza che comprende due o più di quelli sopra elencati.
Malfunzionamento grave	Danneggiamento di un componente hardware o software, oppure degrado delle performance per cause esterne che possa arrecare impatti gravi alla disponibilità di servizio.
Disastro	Qualsiasi evento distruttivo, non provocato direttamente da azione di operatori informatici (es.: blackout, incendio, allagamento, terremoto) in grado di condizionare direttamente l'operatività dei sistemi informatici.

È di fondamentale importanza effettuare una prima valutazione sull'impatto dell'incidente ai fini di indirizzare in modo efficace le risorse necessarie alla sua gestione. Tale attività consiste in una prima classificazione della sua portata in base ad alcuni parametri di seguito elencati:

- il livello di criticità della risorsa ICT coinvolta, determinato in base alle valutazioni inerente la Business Impact Analysis (in caso di coinvolgimento di più risorse verrà assunto come tale quello a maggiore criticità
- il numero di risorse informatiche coinvolte, inteso come numero di server/applicazioni;

- il numero di utenti o postazioni di lavoro potenzialmente impattati dalla indisponibilità del servizio informatico;
- l'eventuale coinvolgimento di risorse ICT/utenti esterni all'organizzazione;
- l'esposizione su Internet del servizio;
- il tipo di danno arrecato (economico, immagine, mancato adempimento normativo ecc.);
- gli enti o le organizzazioni coinvolte nell'incidente;
- l'eventualità di coinvolgere le forze dell'ordine a causa di possibili risvolti di natura penale.

In questa fase il gruppo, coordinato dal Dirigente responsabile del Settore Transizione Digitale deve anche valutare ed accertare la gravità dell'incidente di sicurezza.
Il Gruppo di Coordinamento e di Gestione degli Incidenti assicura la gestione operativa e trasmette agli Organi Direttivi report periodici e, in caso di incidenti significativi, apposita informativa per le valutazioni di competenza.
La decisione sulla significatività NIS2 è formalizzata in un'apposita checklist e non dipende automaticamente dal livello interno di gravità. Sono valutati: grave perturbazione operativa o perdite finanziarie per l'Ente; ripercussioni materiali o immateriali considerevoli su altri soggetti; tipologia prevista dall'Allegato ACN applicabile; durata, estensione, servizi e utenti interessati; compromissione di dati o privilegi; effetti transfrontalieri. In caso di dubbio, il Referente CSIRT è coinvolto immediatamente e la valutazione è aggiornata con le nuove evidenze.

GRAVITÀ INCIDENTE DI SICUREZZA	DESCRIZIONE
L3-L4 (Alta/Critica)	Il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il ripristino è di medio o lungo periodo. L'incidente presenta una tra le seguenti condizioni: • Danni a persone e rilevanti perdite di produttività • Compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni confidenziali • Siti web violati o utilizzati a fini di propagazione di materiale terroristico o pornografico • Frode o attività criminale che coinvolga servizi forniti dall'Ente • Impossibilità tecnica di fornire uno o più servizi critici a un elevato numero di utenti per un intervallo di tempo superiore ai 30 minuti nell'arco di una giornata • Impossibilità tecnica di fornire uno o più servizi di criticità media per un periodo di tempo superiore ai 2 giorni lavorativi • Significativa perdita economica, di immagine e/o reputazione nei confronti del pubblico o degli utenti
L2 (Media)	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta". Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza. Il ripristino ha tempi che non compromettono la continuità del servizio L'incidente presenta una tra le seguenti condizioni: • Compromissione di server • Degrado di prestazioni relativo ai servizi con conseguente perdita di produttività da parte degli utilizzatori

GRAVITÀ INCIDENTE DI SICUREZZA	DESCRIZIONE
	• Attacchi che provocano il funzionamento parziale o intermittente della rete • Impossibilità tecnica di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori ai 30 minuti di tempo ripetuti su più giornate • Impossibilità tecnica di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti nell'arco di una o più giornate • Basso impatto in termini di perdita economica, di immagine e/o reputazione nei confronti degli utenti
L1 (Bassa)	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta o media". Non vengono compromessi asset o servizi. L'incidente presenta le seguenti condizioni: • Interruzione dell'attività lavorativa di un numero ristretto di dipendenti e per un breve periodo di tempo. • Contaminazioni da virus in un medesimo sito ma comunque identificate dai sistemi anti-malware • Nessuna o limitata perdita di operatività o di business da parte di un ridotto numero di dipendenti

Ai fini della coerenza con il Piano di Gestione delle Crisi, la scala operativa è L1-L4: L1 evento limitato senza impatto sui servizi; L2 evento con impatto contenuto su uno o più servizi; L3 interruzione di servizi critici o rischio elevato, con attivazione del Comitato di Crisi e della Business Continuity; L4 grave compromissione o indisponibilità prolungata, con possibile attivazione completa di crisi, BC e DR. I criteri dettagliati e le soglie temporali sono riesaminati con la BIA e il risk assessment. La qualifica di incidente significativo NIS2 resta separata e può ricorrere a qualsiasi livello sulla base dei criteri normativi.

Per alcuni incidenti può risultare difficile assegnare un livello di gravità definitivo prima che l'analisi sia completa; in tal caso occorre valutarla sulla base delle evidenze note sino a quel momento, assumendo che la gravità potrebbe molto probabilmente aumentare nel caso non si effettui alcuna operazione di contenimento.
In ogni caso, è opportuno verificare ciclicamente, nel periodo in cui l'incidente è in corso, la gravità assegnata allo stesso in quanto essa può variare nel tempo.
Al termine della fase di analisi, è necessario informare il Direttore Generale/Segretario Generale.

9.4. COMUNICAZIONE DEGLI INCIDENTI

Tutti i dipendenti sono tenuti a segnalare i potenziali incidenti in modo tempestivo come primo punto di contatto alla struttura organizzativa dell'Ente adibita alla gestione della sicurezza ICT via mail, o attraverso le specifiche modalità adottate dall'Ente.
L'attivazione della conseguente procedura di gestione incidenti di sicurezza sarà quindi a carico del Coordinatore per la gestione degli incidenti di sicurezza che dovrà comunque riportare la situazione al Titolare. Le evidenze raccolte costituiscono base informativa per le comunicazioni e le eventuali notifiche verso le autorità competenti, incluse quelle previste dalla normativa NIS2.

9.4.1. Comunicazione Interna

Viene redatto un messaggio interno che deve includere:

- descrizione dell'incidente
- azioni immediate intraprese
- istruzioni per il personale su come rispondere a domande di clienti o partner
- misure preventive per evitare futuri incidenti simili

Il messaggio viene distribuito al personale attraverso e-mail protetta, messaggi nei sistemi di gestione interna, o riunioni riservate.

Esempio di messaggio:
"Cari colleghi, desideriamo informarvi che si è verificato un incidente di sicurezza. Il nostro team ha già preso misure per limitare l'impatto e stiamo indagando ulteriormente. Vi preghiamo di non rispondere direttamente a eventuali richieste di clienti o fornitori. Aggiornamenti seguiranno a breve. Grazie per la collaborazione."

9.4.2. Comunicazione Esterna

Viene redatto un messaggio esterno, approvato dal gruppo di Coordinamento e di Gestione degli Incidenti e veicolato dalla struttura competente in materia di comunicazione esterna, che deve includere**:**

- descrizione generale e non tecnica dell'incidente
- eventuali rischi e possibili effetti sull'utente
- misure preventive attuate
- dettagli di contatto per ulteriori informazioni

Il messaggio viene distribuito a clienti e fornitori tramite e-mail criptata o portali protetti.

Esempio di Messaggio:
"Gentile XXX, La informiamo che abbiamo identificato e contenuto un incidente di sicurezza che potrebbe aver coinvolto i suoi dati. Abbiamo adottato tutte le misure necessarie per proteggere le informazioni e stiamo migliorando ulteriormente i nostri protocolli di sicurezza. Se desidera ulteriori informazioni o chiarimenti, può contattare il nostro servizio di assistenza al numero …"

9.4.3. Comunicazione Finale

Una volta risolto l'incidente, il Coordinatore per la gestione degli Incidenti di Sicurezza prepara un report conclusivo e comunica la chiusura dell'incidente, sia internamente che esternamente, se necessario.
Messaggio di Chiusura Interno: *"L'incidente di sicurezza segnalato in data … è stato risolto. Ringraziamo tutti per la collaborazione."*
Messaggio di Chiusura Esterno: *"Gentile xxx, desideriamo informarLa che l'incidente di sicurezza è stato risolto. Restiamo a disposizione per ulteriori chiarimenti. Grazie per la fiducia riposta nella nostra organizzazione."*

9.4.4. Comunicazione DATA BREACH

Comunicazione della violazione al Garante

Quando l'incidente comporta una violazione di dati personali, il Titolare notifica la violazione al Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando ne è venuto a conoscenza, salvo che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Se il rischio è elevato, la violazione è comunicata agli interessati senza ingiustificato ritardo, salvo le eccezioni applicabili. La valutazione GDPR è documentata e procede in parallelo e indipendentemente dalla valutazione NIS2.

Comunicazione della violazione agli interessati

Alcune violazioni di dati, quelle che comportano un rischio elevato per i diritti e le libertà delle persone fisiche, devono essere comunicate agli interessati senza ingiustificato ritardo. Tale comunicazione, da redigere in aderenza all'allegato del presente documento, nonché formulata con linguaggio chiaro e comprensibile agli utenti (quindi non in gergo tecnico) deve ricomprendere:

- la descrizione della natura della violazione;
- i recapiti del Data Protection Officer;
- la descrizione delle probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione è indirizzata direttamente agli interessati mediante canali appropriati e tracciabili. Solo quando la comunicazione individuale richiederebbe sforzi sproporzionati può essere utilizzata, previa valutazione documentata del Titolare con il supporto del DPO, una comunicazione pubblica o una misura analoga che informi gli interessati con efficacia equivalente, ai sensi dell'art. 34, par. 3, lett. c), GDPR.

9.4.5. Comunicazione Incidente di Sicurezza al CSIRT

Il Comune notifica senza ingiustificato ritardo al CSIRT Italia ogni incidente significativo.

Codice	Fattispecie di incidente significativo	Descrizione
IS-1	Perdita di riservatezza verso l'esterno di dati digitali	Incidente che determina la perdita di riservatezza di dati digitali nei confronti di soggetti esterni non autorizzati.
IS-2	Perdita di integrità con impatto verso l'esterno di dati digitali	Incidente che determina l'alterazione o la compromissione dell'integrità di dati digitali, producendo un impatto verso l'esterno.
IS-3	Violazione dei livelli di servizio attesi	Incidente che determina il mancato rispetto dei livelli di servizio attesi.

Il Coordinatore registra il momento di conoscenza e informa immediatamente il Referente CSIRT e i sostituti; la trasmissione è effettuata tramite il servizio dedicato del Portale ACN. Un eventuale canale alternativo è utilizzato solo se previsto o comunicato da ACN/CSIRT Italia e l'indisponibilità del Portale è documentata.

- Entro 24 ore dalla conoscenza: pre-notifica che, ove possibile, indica se l'incidente può

derivare da atti illegittimi o malevoli o avere impatto transfrontaliero.

- Entro 72 ore dalla conoscenza: notifica che aggiorna la pre-notifica e contiene una prima valutazione della gravità e dell'impatto e, ove disponibili, gli indicatori di compromissione.
- Su richiesta del CSIRT Italia: relazione intermedia con gli aggiornamenti pertinenti sulla situazione.
- Entro un mese dalla trasmissione della notifica delle 72 ore: relazione finale contenente almeno:
  - descrizione dettagliata dell'incidente, della gravità e dell'impatto;
  - tipo di minaccia o causa originale (root cause) e misure di attenuazione adottate e in corso;
  - eventuale impatto transfrontaliero. Se l'incidente è ancora in corso alla scadenza, sono trasmesse relazioni mensili sui progressi e una relazione finale entro un mese dalla conclusione della gestione.

Modalità di Segnalazione:

- Trasmissione tramite il Portale ACN, Servizio NIS dedicato alle notifiche, da parte del Referente CSIRT o sostituto abilitato; sono conservati ricevuta, protocollo, versione trasmessa, allegati e timestamp. Non è utilizzata una PEC generica salvo specifica istruzione contingente di ACN/CSIRT Italia.
- Raccordo con il Punto di Contatto NIS, gli Organi di Amministrazione e Direttivi, il DPO e le ulteriori Autorità competenti, secondo la natura dell'incidente e senza ritardare le notifiche obbligatorie.

Per ogni incidente è prevista la produzione e conservazione della seguente documentazione:

- Scheda tecnica dell'incidente (modello AGID);
- Registro incidenti, aggiornato periodicamente;
- Report finale contenente:
  - Descrizione dettagliata dell'incidente;
  - Azioni correttive adottate;
  - Valutazione dell'impatto;
  - Lezioni apprese.

Sentito il CSIRT Italia, se ritenuto opportuno e ove possibile, il Comune comunica senza ingiustificato ritardo ai destinatari dei servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura e, per le minacce significative, le misure correttive o di mitigazione che possono adottare. Ogni comunicazione è approvata secondo le competenze definite, coordinata con il DPO e la Comunicazione Istituzionale e limita la divulgazione di informazioni che possano aggravare il rischio o compromettere indagini.

9.4.6. Comunicazione di informazioni pertinenti al CSIRT

In aggiunta alle notifiche obbligatorie, il Comune può trasmettere al CSIRT Italia, tramite il Referente CSIRT, notifiche volontarie relative a incidenti non significativi, minacce informatiche e quasi-incidenti ai sensi dell'art. 26 del D.Lgs. 138/2024. La decisione è documentata e non sostituisce gli obblighi previsti da altre normative o contratti.

9.5. ATTIVAZIONE DELLA PROCEDURA E MONITORAGGIO DELLE ATTIVITÀ

L'attivazione della procedura di gestione incidenti, mediante le opportune segnalazioni nel flusso, sarà a carico del Coordinatore per la gestione degli incidenti di sicurezza, il quale, a seconda della gravità attribuita in fase di identificazione dell'incidente, utilizzerà diverse modalità di attivazione e tracking.

9.5.1. Incidente di livello L3 o L4 (gravità alta o critica)

Per un incidente L3 o L4 il Coordinatore attiva immediatamente il Gruppo di Coordinamento e, secondo il Piano di Gestione delle Crisi, coinvolge RTD, Direttore Generale/Segretario Generale, Sindaco o delegato, DPO, Comunicazione, responsabili di servizio e fornitori. È predisposto un rapporto iniziale, anche incompleto, senza attendere la conclusione dell'analisi; la possibile significatività NIS2 è valutata e riesaminata contestualmente.
Lo scopo principale di questa prima fase è di attivare il gruppo sicurezza per la gestione dell'incidente ed eventualmente anche informare il DPO per la valutazione di un eventuale data breach. Il Rapporto incidente di sicurezza sarà poi completato in tutte le sue parti in fase di chiusura dell'incidente.

Il Rapporto di incidente e la relativa documentazione sono conservati in un repository protetto, soggetto a backup e ad accesso limitato, per il periodo previsto dal piano di conservazione documentale dell'Ente (in fase di aggiornamento), tenendo conto degli obblighi applicabili, delle esigenze di audit, della prescrizione, di indagini o contenziosi e di eventuali legal hold.
È altresì fondamentale che tutte le operazioni eseguite per la gestione di un eventuale incidente siano opportunamente tracciate (es. strumento informatico di ticketing o altro), permettendo in tal modo di poter identificare tutte le risorse coinvolte nelle operazioni tecniche di gestione e poterle eventualmente indicare in ambito giudiziale come testimoni. Le indagini svolte e le operazioni di gestione formeranno quindi una base dati che andrà ad incrementare la conoscenza dell'Ente in merito agli incidenti di sicurezza informatica.
Nel caso in cui l'incidente di sicurezza abbia un impatto sulla continuità operativa è necessario fare riferimento al piano di Business Continuity ed eventualmente al piano di Disaster Recovery.

9.5.2. Incidente di livello L1 o L2 (gravità bassa o media)

Gli incidenti L1 o L2 possono essere coordinati dalla struttura operativa con informativa al RTD secondo le soglie definite; resta obbligatoria la valutazione NIS2 e GDPR e il coinvolgimento del DPO o del Referente CSIRT quando pertinente.
Ogni incidente, indipendentemente dal livello, è registrato almeno con identificativo, timeline, classificazione, decisioni, sistemi e servizi coinvolti, azioni eseguite, evidenze e chiusura. Per L2-L4, per incidenti NIS2/GDPR, per eventi con possibile rilievo legale o per quelli che richiedono azioni correttive è redatto il Rapporto di Incidente completo. La mancata redazione deve essere motivata e approvata dal Coordinatore.

9.6. CONTENIMENTO, RIMOZIONE E RIPRISTINO

Le operazioni di contenimento hanno due importati fini:

- evitare che il danno si propaghi o almeno limitarne la diffusione;
- acquisire le eventuali evidenze digitali di reato prima che queste possano essere compromesse, ovvero:
  - identificare tutti i sistemi che possono essere stati compromessi o sui cui sia possibile raccogliere eventuali evidenze digitali di reato;
  - effettuare delle copie delle eventuali evidenze digitali di reato in modo valido dal punto di vista forense;
  - documentare in modo dettagliato tutte le operazioni eseguite, onde evitare in un eventuale ambito giudiziale possibili contestazioni sulla correttezza delle operazioni eseguite;
  - eseguire le attività di contenimento con personale qualificato (sistemisti o esperti applicativi) appositamente addestrato/formato.

Prima di intraprendere azioni di contenimento o ripristino che possano alterare lo stato dei sistemi, devono essere raccolte e messe in sicurezza le evidenze rilevanti, in conformità all'Allegato 4.
Tutte le operazioni eseguite saranno comunque sotto la responsabilità del coordinatore della gestione degli Incidenti di sicurezza il quale dovrà riportare nel Rapporto di Incidente:

- data ed ora delle azioni eseguite sui sistemi, applicazioni o dati;
- le generalità delle risorse che hanno materialmente eseguito le operazioni;
- i risultati conseguiti.

Le operazioni di contenimento possono essere di due tipologie: a breve termine e a lungo termine.

9.6.1. Contenimento a breve termine

Le operazioni di contenimento a breve termine mirano a mettere in sicurezza gli eventuali sistemi interessati da un incidente, senza alterarne la configurazione o inquinare eventuali evidenze digitali di reato.
Come esempi di azioni di contenimento a breve termine si possono indicare:

- creazione di regole firewall atte a bloccare l'accesso ai sistemi coinvolti;
- disabilitazione di account utente sui sistemi centralizzati di autenticazione;
- cambio di configurazione sui sistemi DNS;
- disconnessione dei sistemi coinvolti dalla rete mediante riconfigurazione di apparati di rete.

Dopo aver messo in sicurezza i sistemi coinvolti nell'incidente, mediante l'operazione di contenimento a breve termine, è possibile procedere all'acquisizione di eventuali evidenze digitali (es. mediante copia forense dei dischi) oppure procedere con l'esecuzione di normali backup atti a mettere in sicurezza i dati per poterli riutilizzare nella eventuale ricostruzione del sistema colpito dall'incidente.

È necessario procedere all'acquisizione forense delle evidenze digitali di reato in ogni caso in cui si prevede un prosieguo in ambito legale come per esempio:

- accessi abusivi a sistemi o informazioni;

- attività illecite commesse da dipendenti o comunque mediante il sistema Informativo gestito da dell'Ente;
- violazioni della privacy di utenti;
- utilizzo illegale dei sistemi per perpetrare truffe o diffondere materiale illecito.

Quando invece l'incidente è causato da malfunzionamenti o errori umani è possibile procedere eseguendo una normale operazione di backup relativa a dati o configurazioni eventualmente presenti sul dispositivo coinvolto nell'incidente.

9.6.2. Contenimento a lungo termine

Il contenimento a lungo termine comporta l'esecuzione di operazioni tecniche direttamente sui sistemi coinvolti nell'incidente, per questo motivo questa azione deve essere eseguita solo dopo aver messo in sicurezza le evidenze digitali di reato o i dati presenti sul sistema impattato. Tali operazioni mirano a rendere i sistemi coinvolti più sicuri e permettono di lasciarli in attività sino al momento in cui sia possibile procedere ad operazioni più complesse di rimozione delle cause.

Come esempio di operazioni di contenimento a lungo termine si possono elencare:
- installazione di patch o aggiornamenti di sistema e/o applicativi;
- cancellazione di file o dati;
- arresto di servizi o processi malevoli;
- cambio di configurazione di programmi.

Al termine di queste operazioni i sistemi coinvolti nell'incidente non possono ancora dichiararsi sicuri, ma è possibile utilizzarli con le dovute cautele sino a quando non saranno rimosse definitivamente le cause che hanno scatenato l'incidente.

Durante questa fase possono emergere necessità che richiedono l'acquisizione di risorse economiche e operative, come per esempio:
- allocare risorse economiche per la fase di acquisizione forense/backup e le successive fasi di gestione;
- isolare e/o arrestare eventuali servizi o sistemi critici di produzione coinvolti;
- valutare eventuali conseguenze legali;
- relazionarsi con altre Strutture dell'Ente per comunicare eventuali disservizi. In tali casi il Coordinatore per la gestione degli incidenti di sicurezza può operare le corrette scelte in autonomia, comunicando al Gruppo di Coordinamento e di Gestione degli Incidenti di Sicurezza le eventuali azioni che saranno intraprese.

9.6.3. Rimozione

Le operazioni di rimozione sono volte all'eliminazione definitiva del problema o della vulnerabilità utilizzata per compromettere un sistema coinvolto in un incidente e riportarlo ad un livello di sicurezza elevato. Le attività che sono solitamente eseguite in questa fase possono essere di diverso tipo, per esempio:
- aggiornamento di release dei sistemi operativi o del software presente (per rimuovere eventuali vulnerabilità di sicurezza);

- rimozione di eventuali servizi o software che, utilizzati in modo malevolo, possono compromettere il sistema stesso (hardening);
- In alcuni casi, come per le infezioni da virus/malware, può essere più semplice e meno oneroso economicamente, ricostruire l'intera macchina reinstallando il software a partire dal sistema operativo.

Le operazioni di rimozione possono essere particolarmente onerose in quanto potrebbe essere necessario:

- acquisire nuovo hardware o licenze software;
- utilizzare risorse interne o esterne per l'esecuzione delle operazioni di rimozione;
- eseguire dettagliati test di funzionamento sui sistemi e sulle applicazioni interessate dall'incidente.

La valutazione dell'impatto tecnico ed economico delle operazioni di rimozione deve essere eseguita dal gruppo Gestione Sicurezza, eventualmente coinvolgendo tutti i soggetti interessati e fornendo al Coordinatore per la gestione degli incidenti di sicurezza, tramite un report di dettaglio, le indicazioni degli eventuali costi da sostenere e dei tempi necessari al ripristino.
I tempi necessari per poter procedere alla fase di rimozione possono essere relativamente lunghi (anche nell'ordine di 1 o 2 settimane) a causa delle necessità di approvvigionamento sopra descritte, ma non possono protrarsi all'infinito in quanto l'operazione di contenimento a lungo termine non è da considerarsi risolutiva del problema, ma solo ed esclusivamente un'azione a titolo temporaneo.

9.6.4. Ripristino

Il ripristino avviene in condizioni controllate e sicure: sono verificate integrità di dati e configurazioni, rimozione della persistenza, vulnerabilità e credenziali compromesse, logging e monitoraggio, segregazione degli accessi privilegiati e disponibilità di copie affidabili. Per eventi cyber rilevanti si applicano clean recovery e criteri di accettazione concordati con i responsabili di servizio; eventuali scostamenti da RTO/RPO o controlli minimi sono documentati e approvati.
In questa fase le operazioni eseguite mirano principalmente a verificare che i sistemi coinvolti nell'incidente siano stati correttamente riattivati e che siano nuovamente sicuri, per considerare l'incidente effettivamente chiuso.
È necessario ottenere un elevato grado di certezza che quanto accaduto non possa ripetersi, per questo motivo si rende necessario definire con il dovuto dettaglio tutte le fasi di riattivazione di un sistema coinvolto, sia nei modi che nei tempi attesi per il ripristino, sia nei controlli da effettuare per certificare il ritorno alla normalità.

9.7. ATTIVITÀ POST-INCIDENTE

La decisione del momento in cui un sistema coinvolto in un incidente possa ritornare in produzione è in carico al Coordinatore per la gestione degli incidenti di sicurezza che definisce un piano di riattivazione dei diversi servizi impattati dall'incidente.

In alcuni casi specifici può essere necessario riattivare i sistemi in un periodo non lavorativo (es. nelle ore notturne oppure nei fine settimana) per dare la possibilità alle strutture che

hanno in carico la gestione dei sistemi stessi di operare senza che siano presenti richieste di accesso da parte di utenti che non siano quelli deputati all'esecuzione di eventuali test di funzionamento.

Onde verificare che le operazioni di ripristino siano avvenute correttamente si rende necessario monitorare il corretto funzionamento dei sistemi per un periodo di tempo adeguato, per cui potrebbe esservi la necessità di attivare ulteriori controlli utilizzando gli strumenti di monitoraggio in uso, oppure aumentando il livello di profondità degli eventi da registrare nei file di log applicativi o dei sistemi operativi. Sarà il referente per la sicurezza informatica a richiedere la modifica o l'implementazione di nuove regole di monitoring ai soggetti preposti.

Tutti gli incidenti di sicurezza devono essere documentati. Tale documentazione, unitamente alle evidenze degli incidenti, devono essere debitamente archiviate.
In particolare, i data breach devono essere documentati e archiviati in modalità distinguibile rispetto agli incidenti di sicurezza, anche quando la violazione è improbabile che comporti un rischio per i diritti e le libertà delle persone fisiche e pertanto non debba essere notificata all'Autorità Garante e/o agli interessati.

Dal punto di vista tecnico le operazioni di chiusura dell'incidente consistono nella dichiarazione della fine dello stato di incidente e nella compilazione del report relativo all'incidente stesso da parte del referente per la sicurezza informatica.

Il report, firmato digitalmente dal Coordinatore tramite procedura di hashing a garanzia della sua integrità, dovrà essere consegnato al gruppo sicurezza e dovrà essere inviato in forma riservata sotto forma di relazione sull'esito dell'incidente di sicurezza al Sindaco e al Direttore Generale/Segretario Generale.
Il Rapporto conclusivo è conservato nel repository ad accesso controllato per il periodo approvato nel piano di conservazione documentale e, ove necessario, fino alla chiusura di indagini, contenziosi, azioni correttive o legal hold.

In seguito alla chiusura dell'incidente dovranno essere valutate tutte le operazioni eseguite per la gestione dello stesso, evidenziando sia i punti in cui queste sono state eseguite in armonia con le procedure e le aspettative, sia eventuali problemi sorti durante lo svolgimento delle operazioni.
Le informazioni raccolte durante la gestione dell'incidente dovranno essere archiviate, in forma anonimizzata nella knowledge base dell'Ente (consultabile ad accesso ristretto in base al ruolo ricoperto nel processo di gestione incidenti). Le evidenze raccolte e conservate ai sensi dell'Allegato 4 sono parte integrante del rapporto di incidente e sono utilizzate per attività di riesame, audit e miglioramento continuo.

È fondamentale che i punti critici rilevati durante l'esecuzione delle operazioni siano immediatamente condivisi con i componenti del gruppo Gestione Sicurezza e si provveda nel più breve tempo possibile a predisporre quanto può essere necessario per eliminarli o mitigarli, migliorando quindi sia la procedura tecnica di gestione, sia la capacità di operare della struttura preposta, sia le infrastrutture e i sistemi.
Le azioni post-incidente comprendono root cause analysis, verifica dell'efficacia delle misure, aggiornamento di threat intelligence, Valutazione del rischio, Piano di Trattamento,),

configurazioni, contratti e fornitori, Piano di Adeguamento, Piano di Formazione, BC/DR e Piano di Crisi. Ogni azione ha responsabile, priorità, scadenza, evidenza di completamento e verifica di efficacia; i rischi residui sono sottoposti all'accettazione dell'autorità competente.
Di seguito alcuni esempi di punti critici che possono essere rilevati:

- mancanza delle competenze tecniche per operare correttamente su un sistema o applicazione;
- mancanza degli opportuni strumenti tecnici;
- errori nella valutazione della gravità dell'incidente o nelle sue capacità di diffusione;
- errori o difficoltà nell'interazione con soggetti interni;
- errori nella comunicazione verso terze parti o verso dipendenti e collaboratori.

In particolare, può essere utile porsi le seguenti domande:

- La procedura di gestione incidenti è stata correttamente eseguita? È risultata adeguata al contesto?
- Si sono presentati aspetti che hanno rallentato la risoluzione dell'incidente?
- Si sono rilevati elementi che si ritiene siano da cambiare in modo da rendere il processo di gestione degli incidenti più efficace ed efficiente?
- È necessario aggiornare il metodo di analisi della gravità a valle dell'incidente?
- Sono necessarie delle azioni correttive da intraprendere in fase di mitigazione dei rischi onde evitare che l'incidente possa riaccadere?
- È necessario modificare le policy dal punto di vista tecnico (es.: aggiungere file con una determinata estensione tra quelli bloccati dal sistema antivirus)?
- È necessario aggiornare e/o migliorare gli interventi formativi al fine di istruire il personale aziendale sulle problematiche inerenti la sicurezza e la privacy dei dati?
- Sono necessarie risorse addizionali (es.: personale, tools, strumenti hardware o software) per rendere il processo di gestione degli incidenti più efficace ed efficiente?
- Sono necessarie modifiche e/o riconfigurazioni del software (es.: aumentare frequenza di aggiornamento delle firme dei software antivirus e/o antintrusione e, modificare il livello di dettaglio fornito dai sistemi di difesa perimetrali)?

Questa operazione ha lo scopo di verificare che il processo di gestione incidenti sia risultato adeguato a fronteggiare la situazione e far sì che le considerazioni che ne sono scaturite diventino patrimonio comune.
Per questo motivo occorre che entro breve termine dalla chiusura formale di un incidente, il Responsabile per la gestione degli incidenti di sicurezza convochi tutte le risorse che sono state parte attiva nella gestione, con l'obiettivo di valutare collegialmente l'efficacia della procedura di gestione degli incidenti e scrivere in un apposito verbale le considerazioni e le operazioni che possono portare a migliorare l'intera procedura.
Per gli incidenti L3-L4 o significativi è predisposto un riesame formale da trasmettere agli Organi di Amministrazione e Direttivi, contenente timeline, impatti, notifiche e comunicazioni, efficacia della risposta, cause, scostamenti, rischi residui, azioni correttive e risorse necessarie. Il termine interno per il riesame è definito senza pregiudicare la relazione finale NIS2.

9.8. FORMAZIONE E SENSIBILIZZAZIONE

Per garantire l'efficacia della procedura è previsto un piano di formazione continuo per tutto il personale, che include:
La formazione è coordinata con il Piano di formazione e comprende, per RTD, Gruppo Incidenti, Punto di Contatto, Referente CSIRT e sostituti, almeno una esercitazione annuale sulle notifiche 24/72 ore/un mese, sulla valutazione di significatività, sull'uso del Portale ACN, sulla conservazione delle evidenze e sul coordinamento con GDPR, crisi, BC e DR. Partecipazione, esiti e azioni di recupero sono registrati.

- Sessioni formative periodiche;
- Simulazioni di gestione incidenti (esercitazioni tabletop);
- Campagne di sensibilizzazione (es. phishing awareness);
- Aggiornamenti normativi e tecnici.

9.9. REVISIONE E AGGIORNAMENTO DELLA PROCEDURA

La presente procedura viene sottoposta a revisione:

- Almeno una volta l'anno;
- Ogniqualvolta intervenga un cambiamento normativo rilevante;
- A seguito di un incidente significativo o di una lezione appresa rilevante;
- In caso di variazione sostanziale del perimetro tecnologico o organizzativo.

Le versioni aggiornate vengono approvate dagli Organi di Amministrazione e Direttivi e condivise con tutte le funzioni interessate.

9.9.1. INFORMAZIONI DOCUMENTATE

INFORMAZIONE DOCUMENTATA	RESPONSABILE	PERIODICITÀ	ARCHIVIAZIONE	
			METODI	TEMPI
Rapporto incidente di sicurezza	Responsabile IT	N.A.	Archiviazione elettronica (Content Management Database)	In conformità con le normative vigenti
Database incidenti di sicurezza	Responsabile IT	N.A.	Archiviazione elettronica (Content Management Database)	In conformità con le normative vigenti
Consuntivo incidenti di sicurezza	Responsabile IT	1 anno	Archiviazione elettronica (Content Management Database)	In conformità con le normative vigenti
Checklist significatività NIS2 e valutazione GDPR	Coordinatore / Referente CSIRT / DPO per competenza	Per ogni incidente pertinente	Fascicolo elettronico ad accesso controllato	Secondo piano di conservazione e legal hold (in fase di aggiornamento)
Pre-notifica, notifica, relazioni intermedie/finali e	Referente CSIRT o sostituto	Per ogni notifica	Fascicolo incidente / repository protetto	Secondo obblighi applicabili e

INFORMAZIONE DOCUMENTATA	RESPONSABILE	PERIODICITÀ	ARCHIVIAZIONE	
			METODI	TEMPI
ricevute Portale ACN				piano di conservazione
Verbale post-incidente e piano azioni correttive	RTD / Gruppo Incidenti	L2-L4 o quando richiesto	Fascicolo incidente / repository protetto	Secondo piano di conservazione

La registrazione di tutti gli incidenti di sicurezza che si rilevano durante la normale attività dell'azienda costituisce una metrica molto importante per il Sistema di Gestione della Sicurezza delle Informazioni.

La consuntivazione periodica degli incidenti di sicurezza, consistente nella valutazione del numero, della gravità e della tipologia degli incidenti, è un importante strumento di monitoraggio dell'efficacia del modello organizzativo e di governo per la gestione della sicurezza delle informazioni e della cybersicurezza e del SGSI predisposto dalla società partecipata IT.CITY S.p.A. di concerto con l'Ente; deve essere effettuata con cadenza almeno annuale, ed è un elemento di ingresso del Riesame del Sistema, indispensabile per la definizione periodica delle azioni di miglioramento e per l'individuazione dei nuovi obiettivi.
Sono monitorati almeno numero e tipologia degli eventi, distribuzione L1-L4, tempo di rilevamento e contenimento, tempo dal momento di conoscenza all'escalation e alle notifiche, rispetto di RTO/RPO, completezza delle evidenze, recidiva, coinvolgimento dei fornitori, chiusura delle azioni correttive ed efficacia delle misure.

ALLEGATO 1: Istruzioni per gli utenti per la segnalazione dell'incidente

Nel caso di un qualsiasi incidente di sicurezza delle informazioni gli utenti devono prontamente attivarsi per:

- Mitigare gli effetti dell'incidente
- Segnalare l'accadimento dell'incidente all'Help Desk Team
- Collaborare per la soluzione dell'incidente

Mitigare gli effetti dell'incidente

L'utente deve attivarsi nel più breve tempo possibile per impedire che un evento comprometta le informazioni. A titolo esemplificativo nel caso di attacco di un virus

1. Scollegare immediatamente il PC dalla rete
2. Acquisire le informazioni rilevanti (sintomi, messaggi, etc.)
3. Spegnere il PC

Segnalare l'accadimento dell'incidente all'Help Desk Team

Tutti gli incidenti di sicurezza devono essere immediatamente comunicati attraverso

- l'indirizzo di posta elettronica servizi.informatici@comune.parma.it
- il sistema di ticketing Help Desk
- l'indirizzo di posta elettronica sos@itcity.it
- il numero telefonico dell'HelpDesk: 0521 464346 (interno breve 7333)

Collaborare per la soluzione dell'incidente

È necessario assicurare all'Help Desk Team tutto il supporto necessario per consentire la comprensione del problema.

In ogni caso dovranno essere fornite le seguenti informazioni:

- Nome del dipendente
- Tipo di informazioni/dati coinvolti
- Luogo dell'incidente
- Numero di inventario dei dispositivi coinvolti
- Data e ora

ALLEGATO 2: TEMPLATE MODULO Rapporto incidente di sicurezza

1. **Premessa:**

Identificativo univoco; data/ora della segnalazione; data/ora del momento di conoscenza; fonte e soggetto che ha effettuato la prima valutazione.
Livello L1-L4 iniziale e aggiornato; qualificazione NIS2 (sì/no/in valutazione) con motivazione e Allegato ACN applicato; valutazione GDPR e coinvolgimento del DPO.
Referente CSIRT e sostituto coinvolti; timestamp e protocolli di pre-notifica 24 ore, notifica 72 ore, relazioni intermedie/finali; eventuali comunicazioni ai destinatari e alle altre Autorità.
(breve descrizione dell'incidente, dei sistemi coinvolti, degli utenti su cui l'incidente ha impatto, della durata dell'incidente, delle modalità attraverso le quali si è venuti a conoscenza dell'incidente)

2. **Descrizione dettagliata dell'incidente:**

(causa che ha determinato l'incidente); (sistemi coinvolti);
(eventuali disservizi causati); (utenti coinvolti);
(eventuali enti esterni coinvolti);
(dettagli tecnici rilevanti: es. log dei sistemi, traffico di rete, schermate, e- mail, ecc.).
Indicatori di compromissione; sistemi, servizi, cloud e fornitori/subfornitori coinvolti; impatto transfrontaliero; evidenze e catena di custodia; attivazione di crisi, Business Continuity o Disaster Recovery; RTO/RPO effettivi e controlli di sicurezza verificati al ripristino.

3. **Rilevazione dell'incidente:**

(modalità attraverso le quali si è venuti a conoscenza dell'incidente:
- *notifica automatica tramite sistemi di rilevazione*
- *individuazione a seguito di verifiche di sicurezza*
- *segnalazione da parte di un utente*
- *altro.*

4. **Contromisure adottate**

(descrizione delle azioni intraprese per contenere i danni causati dall'incidente e per ripristinare i sistemi)

5. **Conclusioni**

(impatto dell'incidente sui sistemi o sui servizi);
(elementi che avrebbero consentito di prevenire il verificarsi dell'incidente); causa accertata o probabile; misure di attenuazione adottate e in corso; rischi residui; azioni correttive con responsabile e scadenza; aggiornamenti a Piano di Trattamento/Adeguamento, formazione, contratti e procedure.
(ulteriori azioni di approfondimento necessarie).

6. **Note**

(eventuali considerazioni sull'incidente, suggerimenti, adeguamenti da effettuare, ecc.).

7. Riferimenti

(eventuali riferimenti ad allegati o altri documenti).

….. , li …….. per il Gruppo di Coordinamento
e di Gestione degli Incidenti
(nome e cognome)

ALLEGATO 3: DATABASE INCIDENTI SICUREZZA

Gli incidenti di sicurezza devono essere registrati in forma strutturata in un apposito database, che costituisce l'Allegato 3 della presente procedura e consente la tracciabilità del ciclo di vita e degli adempimenti correlati.

Ciascun evento è caratterizzato da:

- Numero progressivo
- Data apertura incidente
- Data e ora del momento di conoscenza e relativa fonte
- Decisione sulla significatività NIS2, motivazione, Allegato ACN applicabile e timestamp delle rivalutazioni
- Valutazione data breach GDPR e decisioni di notifica/comunicazione
- Timestamp e protocolli delle notifiche al CSIRT Italia e delle comunicazioni ai destinatari
- Classificazione operativa L1-L4 e relative variazioni nel tempo
- Tipo incidente (per es.: Guasto, Interruzione servizio, Non osservanza politiche, …)
- Descrizione incidente (spiegare più in dettaglio che cosa è accaduto)
- Cause incidente
- Azione correttiva (si/no)
- Descrizione dell'azione correttiva
- Lesson Learned (interrogarsi su che cosa ci ha insegnato l'incidente)
- Costi diretti o indiretti (valutare l'impatto dell'incidente, per es.: downtime, disservizi, costi aggiuntivi, …)
- Servizi, utenti, sedi, fornitori e subfornitori coinvolti; eventuale impatto transfrontaliero
- Attivazione di Piano di Crisi, Business Continuity o Disaster Recovery e scostamenti da RTO/RPO
- Azioni correttive, responsabili, scadenze, stato e verifica di efficacia
- Impatto sul ciclo lavorativo aziendale (per es.: 4 ore senza internet, 1 giorno downtime LN, ecc…)
- Data chiusura dell'incidente (l'incidente può essere considerato chiuso solo quando si è conclusa l'azione correttiva)

ALLEGATO 4: Regole per l'identificazione, la raccolta e la conservazione delle prove

(ISO/IEC 27001:2022 – d.lgs. 138/2024 NIS2)

1. Scopo

Il presente allegato definisce le regole operative per:

- l'identificazione delle prove (evidenze) relative a incidenti di sicurezza delle informazioni;
- la loro corretta raccolta;
- la conservazione, protezione e tracciabilità delle evidenze;

al fine di garantirne:

- l'integrità,
- l'affidabilità,
- l'utilizzabilità in ambito investigativo, forense, disciplinare e giudiziario, in conformità a ISO/IEC 27001:2022 e al d.lgs. 138/2024 (NIS2).

2. Ambito di applicazione

Le presenti regole si applicano a:

- tutti gli **incidenti di sicurezza**;
- **data breach** ai sensi del GDPR;
- **incidenti significativi NIS2** notificati o notificabili ad ACN/CSIRT;
- incidenti che possano avere **rilievo disciplinare, civile o penale**.

3. Definizione di prova / evidenza

Per **prova (evidenza)** si intende qualsiasi informazione, dato o oggetto, in formato digitale o fisico, idoneo a:

- ricostruire la dinamica dell'incidente;
- individuare cause, responsabilità e impatti;
- supportare decisioni tecniche, organizzative o legali.

Esempi di evidenze:

- log di sistema e applicativi;
- immagini forensi di dischi o memorie;
- file di configurazione;
- email, ticket, segnalazioni;
- screenshot, dump di memoria;
- documentazione cartacea.

4. Principi Fondamentali della Conservazione

Ogni attività di gestione delle prove deve attenersi ai seguenti principi:

- **Integrità:** La prova non deve essere alterata durante la raccolta.
- **Autenticità:** Deve essere possibile dimostrare la provenienza della prova.
- **Tracciabilità (Chain of Custody):** Ogni passaggio di mano o analisi della prova deve essere documentato.

5. Principi fondamentali (ISO/IEC 27001:2022)

La gestione delle evidenze deve rispettare i seguenti principi:

1. **Integrità** – le prove non devono essere alterate;
2. **Tracciabilità** – ogni accesso o operazione deve essere registrato;
3. **Minimizzazione** – raccogliere solo ciò che è necessario;

4. **Riservatezza** – accesso limitato ai soli soggetti autorizzati;
5. **Ripetibilità** – le operazioni devono essere riproducibili e verificabili.

6. Identificazione delle prove

Durante le fasi di **identificazione e analisi dell'incidente**, il referente CSIRT / Team ICT deve:

- individuare i sistemi coinvolti o potenzialmente coinvolti;
- determinare le possibili fonti di evidenza;
- valutare se l'incidente possa avere rilievo:
  - NIS2,
  - GDPR,
  - disciplinare,
  - giudiziario.

In caso di dubbio, **le evidenze devono essere trattate come potenzialmente forensi**.

7. Raccolta delle prove

7.1 Regole operative

La raccolta delle prove deve:

- avvenire **prima** di operazioni distruttive (patch, reinstallazioni, cancellazioni);
- essere effettuata da personale qualificato;
- essere documentata in modo puntuale.

Nota operativa: isolare il sistema dalla rete secondo le istruzioni del gruppo incident response e non spegnerlo, riavviarlo o modificarlo senza una decisione documentata del Coordinatore o dello specialista forense. La priorità tra contenimento immediato e acquisizione dei dati volatili è valutata caso per caso, tenendo conto di propagazione, cifratura in corso, sicurezza delle persone e valore probatorio.

Nel caso di incidenti su infrastrutture gestite da terzi, il Comune richiede formalmente la preservazione e la consegna tempestiva dei log e delle evidenze in formato protetto, secondo i contratti e in tempi compatibili con le notifiche NIS2 e GDPR. Il requisito puntuale e il canale di consegna devono essere verificati e contrattualizzati.

7.2 Tecniche ammesse

- copie forensi bit-stream (preferibili);
- backup completi dei sistemi coinvolti;
- esportazione controllata dei log;
- acquisizione di screenshot e dump;
- raccolta di documentazione e comunicazioni.

Per garantire che la prova non sia stata modificata, ogni file o immagine acquisita deve essere sottoposta a una funzione di **Hash** (es. SHA-256 o SHA-512).

- L'impronta hash deve essere generata immediatamente dopo l'acquisizione.
- Il valore hash deve essere riportato nel "Registro delle evidenze ".

L'acquisizione deve avvenire preferibilmente con strumenti di *forensic imaging* (es. FTK Imager, Autopsy o tool certificati dal fornitore IaaS Lepida) per evitare la modifica delle "date di ultimo accesso" dei file

8. Catena di custodia (Chain of Custody)

Per ogni evidenza deve essere mantenuta una **catena di custodia**, che includa:

- identificativo univoco della prova;
- data e ora di acquisizione;

- soggetto che ha effettuato la raccolta;
- luogo di conservazione;
- ogni accesso, copia o trasferimento;
- data di eventuale distruzione.

La catena di custodia è parte integrante del **Rapporto di Incidente di Sicurezza**.

9. Conservazione delle prove

Le evidenze devono essere conservate:

- in ambienti sicuri, segregati e protetti;
- con controlli di accesso basati su ruoli;
- con meccanismi di protezione dell'integrità (hash, checksum, WORM).

Tempi di conservazione

- **Incidenti con dati personali: conservazione secondo il registro dei trattamenti, il piano di conservazione, la limitazione della finalità, gli obblighi legali e l'eventuale legal hold.**
- **Incidenti con rilievo legale:** fino a chiusura del contenzioso.
- **Conservazione ai fini NIS2 e di vigilanza**
  Le evidenze e la documentazione delle notifiche devono rimanere disponibili, integre e accessibili per dimostrare la corretta gestione dell'incidente e rispondere a richieste di ACN, CSIRT Italia, Autorità giudiziaria o altre Autorità competenti, nel rispetto dei poteri e delle norme applicabili.
  Disponibilità per le Autorità: accesso controllato, tempestivo e tracciato alle evidenze pertinenti, senza alterare la catena di custodia e applicando minimizzazione e riservatezza.
  Tempi di conservazione: l'art. 25 del D.Lgs. 138/2024 non stabilisce un termine generale fisso per tutte le evidenze. Il Comune definisce e approva un piano di conservazione (in fase di aggiornamento) basato su finalità, rischio, obblighi legali, prescrizioni delle Autorità, contenzioso e necessità di audit.

10. Accesso alle evidenze

L'accesso alle evidenze è consentito esclusivamente a:

- Responsabile Sicurezza Informatica / CISO;
- CSIRT / Referente CSIRT/ Team ICT autorizzato;
- DPO (per aspetti GDPR);
- Autorità competenti (ACN, CSIRT, Forze dell'Ordine, Autorità Giudiziaria).

Ogni accesso deve essere **tracciato e motivato**.

11. Integrazione con NIS2

Ai fini del d.lgs. 138/2024:

- le evidenze costituiscono base informativa per:
  - pre-notifica entro 24 ore dalla conoscenza,
  - notifica entro 72 ore dalla conoscenza,
  - relazione finale entro un mese dalla notifica delle 72 ore e relazioni mensili se l'incidente è ancora in corso;
- devono essere rese disponibili ad ACN/CSIRT su richiesta;
- la loro integrità e tracciabilità è elemento essenziale di accountability.

12. Chiusura e distruzione delle prove

Al termine dei tempi di conservazione:

- le evidenze devono essere distrutte in modo sicuro;

- la distruzione deve essere documentata;
- deve essere garantita la non recuperabilità.