COMUNE DI
REGGIO NELL'EMILIA

Gestione degli incidenti di sicurezza relativi alla protezione dei dati personali (Data breach) del Comune di Reggio Emilia

Sommario

1. Premessa

Per violazione di dati personali si intende la violazione di sicurezza (data breach) che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai dati personali comunque trattati.

Una violazione non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, in un incidente (es. un black out, un incendio o una calamità naturale), nella perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione o smarrimento di documenti con dati personali (es. furto o smarrimento di notebook o di smartphone di un dipendente o di fascicoli cartacei giacenti negli uffici comunali o nelle sedi dei Responsabili del trattamento, oppure trattamento non conforme alle regole dell'Ente riguardo la gestione delle credenziali di accesso che provochi una violazione dei dati personali, smistamento di mail con dati personali ad indirizzari errati, pubblicazione errata di atti o informazioni contenti dati personali non pubblicabili, ecc.).

Il presente documento rappresenta lo schema di procedura operativa del Comune di Reggio Emilia per la gestione degli incidenti di sicurezza che possono comportare una violazione di dati personali comunque trattati.

Tali indicazioni operative si applicano tutte le volte che vi sia una violazione di dati personali concreta, sospetta o avvenuta, agli archivi e ai documenti cartacei, ai sistemi informatici e tecnologici, su cui sono conservati dati personali di interessati (cittadini, dipendenti, soggetti terzi, ecc.) che il Comune di Reggio Emilia, o i Responsabili del trattamento nominati dal Comune, trattano.

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni, materiali o immateriali, alle persone fisiche (ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti), discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

La corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati in caso di incidente; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti stessi.

Il presente documento si rivolge al personale, ai Servizi, ai soggetti interni o esterni al Comune, che trattano dati personali di cui il Comune di Reggio Emilia ha la titolarità, in qualunque modo, cartaceo o informatizzato, diretto oppure esternalizzato.

2. Ruoli e responsabilità

Il Comune di Reggio Emilia, con delibera di Giunta ID n° 92 del 22/05/2018 e conseguente atto di nomina del Sindaco Pg. 71191 del 1 giugno 2018 ha formalmente nominato il proprio Responsabile per la protezione dei dati.

Con delibera di Giunta ID n° 156 del 20.09.2018 è stato approvato il "Sistema gestionale del Comune di Reggio Emilia in materia di protezione dei dati personali" che introduce, oltre alle figure obbligatorie previste dal Regolamento europeo (**Titolare**, **Responsabile** e **Responsabile della protezione dei dati**), le figure dei **Coordinatori** (coincidenti con i Dirigenti dell'Ente) e degli Incaricati al trattamento dei dati personali ed istituisce formalmente l'**Ufficio privacy** in capo al "Servizio appalti contratti e semplificazione amministrativa" con compiti di raccordo fra Titolare, Coordinatori e DPO e di supporto ai Servizi dell'Ente per ogni questione inerente l'applicazione del Regolamento europeo 679/2016.

Con il presente documento si stabilisce che all'articolazione del "Sistema gestionale del Comune di Reggio Emilia in materia di protezione dei dati personali" si aggiunge un ulteriore tassello organizzativo individuato nel "**Gruppo di lavoro per la gestione degli incidenti di sicurezza relativi alla protezione dei dati personali (data breach)**" composto dall'Ufficio privacy del Comune di Reggio Emilia e dal personale individuato all'interno del Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi Informativi. E' anche individuato un responsabile del "Gruppo di lavoro per la gestione degli incidenti di sicurezza relativi alla protezione dei dati personali".

I riferimenti nominativi del gruppo, i ruoli, incluso quello di responsabile, gli indirizzi e-mail e numeri di telefono sono elencati nell'Allegato A al presente documento: "Composizione del Gruppo di lavoro per la gestione degli incidenti di sicurezza relativi alla protezione dei dati personali (data breach)".

I responsabili per la gestione della sicurezza informatica sono il Dirigente del Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi Informativi ed il Responsabile della transizione al digitale dell'Ente.

Il responsabile per la gestione della sicurezza dei documenti cartacei è il Dirigente responsabile della gestione documentale dell'Ente.

Il Gruppo di lavoro per la gestione degli incidenti di sicurezza relativi alla protezione dei dati personali (data breach) ha i seguenti compiti:

- rappresentare il punto di riferimento univoco a cui il personale deve rivolgersi per segnalare un potenziale incidente oppure un comportamento sospetto;
- gestire 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;
- garantire che il processo di gestione incidenti sia sempre adeguato alle esigenze dell'Ente, provvedendo che sia sempre aggiornato.

3. Gestione degli incidenti di sicurezza

La segnalazione di un incidente di sicurezza può essere fatta sia da soggetti interni che esterni all'Ente (dipendenti e collaboratori del Comune, Responsabili di trattamento nominati dal Titolare, soggetti interessati o da altre fonti esterne) attraverso i seguenti canali:

- invio mail alla casella privacy@comune.re.it;
- segnalazioni telefoniche o via email ai recapiti indicati nell'Allegato A "Gruppo di lavoro per la gestione degli incidenti di sicurezza e dei Data breach";
- in modo automatico mediante strumenti appositi di Intrusion Detection System (IDS), firewall e antivirus come definiti nel documento "*MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA*" del Comune di Reggio Emilia - ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ e ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE;
- da processi di analisi continuativa degli eventi di sicurezza registrati da vari dispositivi e gestiti, eventualmente in modo centralizzato, attraverso la piattaforma SIEM (security information and event management) specificata nel documento "*MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA*" del Comune di Reggio Emilia - ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ e ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE;

Il "Gruppo di lavoro per la gestione degli incidenti di sicurezza relativi alla protezione dei dati personali", immediatamente convocato dai soggetti individuati nell'Allegato A a seguito delle segnalazioni pervenute, effettua una valutazione dell'evento avvalendosi, nel caso, di altre professionalità necessarie per la corretta analisi della situazione.

Nel corso del processo di valutazione di un incidente di sicurezza il Gruppo potrà essere coadiuvato dal personale dei Servizi del Comune, oppure dal personale dei Responsabili di trattamento nominati o da tutti coloro che il Gruppo riterrà necessario coinvolgere a seconda della tipologia di incidente.

Il "Gruppo di lavoro per la gestione degli incidenti di sicurezza relativi alla protezione dei dati personali" coinvolgerà altresì il Titolare ed i Coordinatori del trattamento dei dati coinvolti nell'incidente di sicurezza per valutare, in relazione alla gravità dell'incidente, le modalità di comunicazioni interne ed esterne. Se durante la gestione dell'incidente emergeranno responsabilità da parte di personale interno al Comune, il Gruppo di lavoro dovrà coinvolgere anche il Servizio di Gestione e Sviluppo del Personale e dell'Organizzazione.

Nelle attività del "Gruppo di lavoro per la gestione degli incidenti di sicurezza relativi alla protezione dei dati personali" deve essere coinvolto il Responsabile della Protezione dei Dati che fornirà il proprio parere sulle valutazioni dell'incidente e in ordine alla necessità di effettuare la notifica al Garante per la protezione dei dati personali.

Sulla scorta delle determinazioni raggiunte, nel caso la violazione comporti un rischio per i diritti e le libertà delle persone fisiche, sarà compito del Titolare, come indicato all'art.33 c.1 del Regolamento europeo 679/2016, notificare la comunicazione dell'avvenuto data breach all'Autorità Garante per la protezione dei dati personali, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il Comune è venuto a conoscenza della violazione, o da quando abbia un ragionevole grado di certezza che si è verificato un incidente di sicurezza che riguardi dati personali. Oltre tale termine, la notifica deve essere corredata delle ragioni del ritardo.

Nell'effettuare le valutazioni degli incidenti di sicurezza e nel determinare le decisioni e le azioni conseguenti, il Titolare del trattamento ed il "Gruppo di lavoro per la gestione degli

incidenti di sicurezza relativi alla protezione dei dati personali" si atterranno scrupolosamente alle disposizioni del Regolamento europeo 679/2016 ed in modo particolare agli articoli 33 e 34.

4. Registro dei Data breach

È istituito, quale Allegato B al presente documento, il "Registro dei data breach" contenente la documentazione di qualsiasi violazione di dati personali, comprese le circostanze ad essa relative, le loro conseguenze ed i provvedimenti adottati per provi rimedio, nonché le scelte e le motivazioni che hanno portato a non notificare l'evento all'Autorità Garante per la protezione dei dati personali.

Dal punto di vista tecnico le operazioni di chiusura di ogni incidente consistono nella dichiarazione della fine dello stato di incidente e della compilazione da parte del responsabile del "Gruppo di lavoro per la gestione degli incidenti di sicurezza relativi alla protezione dei dati personali" di un report firmato digitalmente, protocollato nel software di registrazione di protocollo in uso nell'Ente ed allegato al Registro dei data breach.

Ai sensi dell'Art.33, co. 5 del Regolamento Europeo 679/2016 tale Registro deve essere conservato nell'Ente ed esibito all'Autorità Garante per la protezione dei dati personali in caso di richiesta.

5. Procedura di gestione degli incidenti di sicurezza

La procedura per la gestione degli incidenti di sicurezza ha i seguenti obiettivi:

- 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 di reato sia digitali che materiali;
- valutare eventuali lacune organizzative/tecniche che hanno reso possibile il data breach e proporre azioni per mitigare il rischio di eventi analoghi.

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 intraprendere tutte le operazioni necessarie a garantire la continuità operativa.

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.

6. Identificazione e analisi dell'incidente

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.

6.1 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 a fascicoli cartacei, a reti, sistemi, applicazioni, dati o altre risorse tecnologiche di proprietà dell'Ente 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 o a seguito di sottrazione di fascicoli cartacei.
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 azioni degli operatori (informatici o amministrativi) (es.: black out, incendio, allagamento, terremoto, calamità naturali in genere) in grado di condizionare direttamente l'operatività dei sistemi informatici o di non rendere disponibili i fascicoli cartacei.

Verrà 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 di qualunque risorsa coinvolta, ICT o di altro tipo;
- il numero di risorse coinvolte, se informatiche 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, di 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 di lavoro deve anche stabilire la gravità dell'incidente di sicurezza.

Gravità incidente di sicurezza	**Descrizione**
Alta	Il grado di compromissione di Servizi e/o di sistemi ICT 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 dati personali e 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 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 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
Media	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta". Il grado di compromissione di Servizi e/o di sistemi ICT 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 offerti dall'Ente con conseguente perdita di produttività da parte degli utilizzatori • Attacchi che provocano il funzionamento parziale o intermittente della rete • Impossibilità 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 di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti di tempo nell'arco di una o più giornate ● Basso impatto in termini di perdita economica, di immagine e/o reputazione nei confronti degli utenti
Bassa	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta o media". Non vengono compromessi asset, servizi o sistemi. 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.

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.

6.2 Valutazione dei rischi derivanti dal verificarsi del data breach

Per data breach si intende 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 in qualunque modo trattati.

In caso di data breach il Comune deve valutare i rischi per i diritti e le libertà delle persone fisiche, utilizzando i criteri di seguito indicati:

- la tipologia di violazione, ovverosia il tipo di violazione come declinata nel paragrafo precedente;
- la natura dei dati violati, valutando che più i dati sono "sensibili", maggiore è il rischio di danni per le persone fisiche;
- il volume dei dati violati, considerando che la violazione di diverse tipologie di dati comporta un rischio maggiore rispetto alla violazione di una sola tipologia;
- il numero di individui cui si riferiscono i dati violati, considerando che, generalmente, maggiore è il numero di individui interessati, maggiore è l'impatto di una violazione. Tuttavia, una violazione può avere un impatto grave anche su un solo individuo, a seconda della natura dei dati personali e del contesto in cui è stato compromesso;
- caratteristiche speciali degli individui cui si riferiscono i dati violati, ad esempio minori o persone vulnerabili;
- il grado di identificabilità delle persone, considerato che l'identificazione potrebbe essere possibile direttamente dai dati personali violati senza alcuna ricerca speciale necessaria per scoprire l'identità dell'individuo, oppure potrebbe essere estremamente difficile abbinare i dati personali a un particolare individuo, ma potrebbe comunque essere

possibile a determinate condizioni (sono, quindi, considerati tutti i mezzi di cui ci si possa avvalere per identificare le persone fisiche);

- la gravità delle conseguenze per gli individui: tale criterio è strettamente connesso alla tipologia di dati violati. Deve essere considerato che una violazione di riservatezza può occorrere anche nel caso in cui dei dati personali siano comunicati ad un terzo, pur non autorizzato, ma conosciuto e "fidato". In tali casi, evidentemente la valutazione di tale criterio abbasserà il livello di gravità delle conseguenze per gli individui. Nel caso in cui i dati personali siano nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose il livello di rischio potenziale sarà più elevato.

7. Attività di gestione dell'incidente

7.1 attivazione della procedura e monitoraggio delle attività

L'attivazione della procedura di gestione incidenti, potrà essere effettuata da uno dei membri del Gruppo di lavoro. La gravità attribuita in fase di identificazione dell'incidente, potrà variare durante la fase di analisi iniziale.

Incidente di gravità "Alta"
In caso di incidente di gravità "Alta" il gruppo di lavoro informerà immediatamente il DPO.
Il Rapporto sull'incidente di sicurezza sarà poi completato in tutte le sue parti in fase di chiusura dell'incidente.
E' altresì fondamentale che tutte le operazioni eseguite per la gestione di un eventuale incidente siano opportunamente tracciate (attraverso lo strumento informatico di ticketing in uso all'Ente o altro strumento che attesti la segnalazione).

Incidente di gravità "Media" o "Bassa"
In caso di incidente di gravità "Media o Bassa", l'incidente può essere completamente gestito dal Responsabili indicati nel Gruppo di lavoro di cui all'Allegato A, fermo restando il coinvolgimento del DPO. Se l'incidente è di natura informatica spetterà al Dirigente del Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi Informativi ed al Responsabile della transizione al digitale dell'Ente. Se l'incidente coinvolge documenti cartacei spetterà al Dirigente responsabile della gestione documentale dell'Ente. Solo in caso di data breach, è obbligatoria la stesura del Rapporto di incidente di sicurezza e la tracciatura delle operazioni eseguite.

7.2 gestione dell'incidente

Tutte le operazioni eseguite sono sotto la responsabilità del Responsabile del Gruppo di lavoro di cui all'Allegato A.

Vengono definite due casistiche principali:

1. 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. Questa operazione potrà quindi essere eseguita utilizzando i sistemi ed i programmi utilizzati per effettuare le comuni operazioni di backup ed hanno lo scopo di mettere in sicurezza le informazioni necessarie per una eventuale reinstallazione del dispositivo.

2. l'incidente è causato da un attacco informatico, accesso abusivo, ecc:
   in questo caso si procederà con i passi indicati sotto

7.2.1 Contenimento a breve termine

Occorre svolgere azioni volte a mettere in sicurezza i sistemi compromessi evitando la diffusione del danno ed evitando il più possibile l'alterazione delle configurazioni o la compromissione di informazioni importanti per la comprensione di quanto accaduto o per l'acquisizione di evidenze digitali di reato.

Come esempi di azioni di contenimento a breve termine si possono indicare:

- creazione/modifica di regole del 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.

7.2.2 Acquisizione di informazioni sull'incidente

Dopo aver messo in sicurezza i sistemi coinvolti nell'incidente, mediante l'operazione di contenimento a breve termine, è possibile procedere all'acquisizione di informazioni su quanto accaduto sia per eventuali fini legali che per pianificare azioni per ridurre il rischio di ripetizione dell'incidente.

Come esempi di azioni di contenimento a breve termine si possono indicare:

- copie di documenti, archivi, configurazioni coinvolti nella compromissione
- copie dei log dei sistemi coinvolti
- documentazione dettagliata dei sintomi/malfunzionamenti rilevati

7.2.3 Soluzione temporanea

L'attivazione di una soluzione temporanea comporta l'esecuzione di operazioni tecniche direttamente sui sistemi coinvolti nell'incidente.
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 temporaneamente sino a quando non sia possibile procedere con le operazioni di rimozione definitiva di quanto ha scatenato l'incidente.

7.2.4 Soluzione definitiva

Queste attività 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 per l'attivazione della soluzione definitiva 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;
- richiedere adeguamenti applicativi molto impattanti sia dal punto di vista economico che organizzativo

La valutazione dell'impatto tecnico ed economico delle operazioni di soluzione definitiva deve essere eseguita dal gruppo di lavoro di cui all'Allegato A, eventualmente coinvolgendo tutti i soggetti interessati e fornendo al Titolare informazioni sugli eventuali costi da sostenere e dei tempi necessari. Il gruppo di gestione della sicurezza dovrà pertanto concordare una road-map per l'attivazione della soluzione definitiva con tempi che potranno anche essere lunghi.

8. Disposizioni finali e transitorie

1. L'approvazione e la revisione del presente documento "Gestione degli incidenti di sicurezza relativi alla protezione dei dati personali (Data breach)" è di competenza della Giunta.

2.Il Dirigente del Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi Informativi aggiorna con propria determinazione gli allegati al presente documento.

3. Per quanto non espressamente previsto dalle presenti documento "Gestione degli incidenti di sicurezza relativi alla protezione dei dati personali (Data breach), si rinvia al Regolamento europeo 679/2016 in materia di protezione dei dati personali, nonché alle altre disposizioni normative vigenti in materia e successive modificazioni ed integrazioni.