



Comune di Sestola
Provincia di Modena
C.so Umberto I, 5- 41029 Sestola (MO)
Tel 0536/62743
comune@cert.comune.sestola.mo.it

Procedura di gestione degli Incidenti di Sicurezza **(DATA BREACH)**

..

Approvato con Deliberazione di G.C. n. 9 del 05 Marzo 2020

Sommario

[Premessa](#)

[Incidente di Sicurezza](#)

[Data breach ai sensi del GDPR](#)

[Notifica al Garante e agli interessati](#)

[Ruoli e Responsabilità](#)

[Procedura di gestione degli incidenti di sicurezza](#)

[Dettagli della procedura di gestione degli incidenti di sicurezza:](#)

[Preparazione](#)

[Identificazione e analisi dell'incidente](#)

[Gestione del data breach](#)

[Valutazione dell'impatto dell'incidente](#)

[Valutazione dei rischi derivanti dal verificarsi del data breach](#)

[Comunicazione degli incidenti](#)

[Attivazione delle procedure di gestione degli incidenti e monitoraggio delle attività](#)

[Contenimento, rimozione e ripristino:](#)

[Contenimento a breve termine](#)

[Contenimento a lungo termine](#)

[Rimozione](#)

[Ripristino](#)

[Attività post-incidente](#)

PREMESSA

Il presente documento rappresenta il riferimento del Comune di Sestola per la regolamentazione della gestione degli incidenti di sicurezza informatica che possono occorrere ai servizi ed ai dati gestiti.

La corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati dell'organizzazione 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.

Inoltre, con specifico riferimento all'obbligo di cui all'art. 33 del Regolamento UE n. 679/2016, il presente documento individua quali siano le violazioni che ricadono nell'ambito della suddetta normativa, i casi in cui l'Ente deve notificare i data breach all'Autorità Garante ed agli interessati, le misure atte a trattare il rischio e la documentazione da produrre.

Si rappresenta che l'art. 32 del Regolamento UE 679/2016 dispone che devono essere approntate misure tecniche e organizzative adeguate per 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.

L'ambito di applicazione è rappresentato da sistemi ICT dell'Ente e vengono presi in considerazione incidenti che possono scaturire sia attraverso l'azione di un attacco informatico portato da elementi esterni all'organizzazione sia generati da un eventuale comportamento negligente o scorretto, di natura ostile con obiettivi frodatori da parte di un collaboratore dell'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 UE 69/2016 trova applicazione nei soli casi in cui la violazione riguardi dati personali, come definiti dall'art. 4 n.1 ("dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile).

Il presente documento è applicabile alle risorse ed ai servizi di tipo informatico gestiti in modo diretto oppure esternalizzato da parte del Comune di Sestola ed anche, nelle parti compatibili, in presenza di possibili violazioni di dati personali contenuti in banche dati cartacee.

Per le specifiche relative all'organizzazione dell'Ente, si rinvia al "Modello organizzativo in materia di protezione dei dati personali" approvato con deliberazione di G.C. n.66 del 26/05/2018.

INCIDENTE DI SICUREZZA

Ai sensi del presente documento, per incidente di sicurezza deve intendersi *"la violazione, la minaccia imminente di violazione di una politica di sicurezza informatica, di politiche di utilizzo accettabili o di prassi standard di sicurezza, correlato ad una violazione di dati o informazioni"*. Esempi di incidenti sono:

- 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.

DATA BEACH AI SENSI DEL GDPR

Il Regolamento UE 679/2016 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.

Gli effetti di una violazione possono causare danni fisici, materiali o immateriali, ovverosia la perdita del controllo sui propri dati personali, la limitazione dei loro diritti, discriminazione, furto d'identità o frode, perdita finanziaria, inversione non autorizzata di pseudonimizzazione, danno alla reputazione e perdita di riservatezza dei dati personali protetti dal segreto professionale . Può anche includere qualsiasi altro significativo svantaggio economico o sociale per tali individui.

NOTIFICA AL GARANTE E AGLI INTERESSATI

In caso di data breach l'Ente deve valutare i rischi per i diritti e le libertà delle persone fisiche, registrando le evidenze di tale analisi.

Nell'eventualità che tale valutazione rappresenti elementi di rischio per i diritti e le libertà delle persone fisiche l'Ente effettua la notifica al Garante delle violazioni di dati personali.

Quando le violazioni di dati comportano un rischio che viene valutato come elevato per i diritti e le libertà delle persone fisiche, le stesse devono essere comunicate agli interessati senza ingiustificato ritardo, fornendo loro specifiche informazioni in ordine alle salvaguardie che devono adottare per proteggere loro stessi dalle conseguenze della violazione.

Questo rischio esiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone i cui dati sono stati violati. Tale rischio è presunto quando il data breach riguarda le categorie particolari di dati di cui all'art. 9 del Regolamento UE 679/2016.

I criteri che devono guidare la valutazione del suddetto rischio sono i seguenti:

- la tipologia di violazione
- la natura dei dati violati
- il volume dei dati violati
- il numero di individui cui si riferiscono i dati violati
- caratteristiche speciali degli individui cui si riferiscono i dati violati
- il grado di identificabilità delle persone
- la gravità delle conseguenze per gli individui

La valutazione deve essere condotta secondo una metodologia operativa adeguata che viene dettagliata nel seguito.

L'Ente notifica la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è stata rilevata. Oltre tale termine, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni sono fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il termine principia dal momento in cui l'Ente ha consapevolezza della violazione di dati, ovverosia quando si raggiunge un ragionevole grado di certezza che si è verificato un incidente di sicurezza che ha compromesso i dati personali.

L'Ente può tardare la notifica all'Autorità Garante, nei casi in cui tale notifica possa produrre effetti negativi sugli individui.

Nei casi in cui l'Ente disponga di informazioni solo parziali della violazione, viene, comunque, effettuata la notifica al Garante.

Il Garante per la protezione dei dati personali può richiedere, in ogni caso, la notifica della violazione agli interessati.

La comunicazione della violazione agli interessati può essere ritardata nei casi in cui tale comunicazione possa pregiudicare le indagini su cause, natura e conseguenze della violazione, anche su indicazione delle varie Autorità di controllo.

L'Ente utilizza lo strumento più efficace affinché tale notifica sortisca il maggiore effetto possibile.

RUOLI E RESPONSABILITA'

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.

L'Ente istituisce un **Gruppo per la Gestione della Sicurezza ICT**, composto dal soggetto esterno cui è affidato il Servizio ICT per l'Ente e dal personale appositamente incaricato dell'Area Tecnica e dell'Area Urbanistica, con il controllo e il coordinamento degli stessi. Questo gruppo ha le seguenti competenze:

- rappresentare il punto di riferimento univoco a cui il personale dell'organizzazione 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.

I riferimenti del gruppo (nominativi, indirizzo e-mail, numero di telefono ecc.) devono essere ben identificati e facilmente raggiungibili.

Il personale appositamente incaricato nell'Area Tecnica e Urbanistica rappresenta i **referenti per la gestione della sicurezza informatica** e saranno le figure che avranno in carico la gestione degli incidenti.

Nel corso del processo di gestione di un incidente di sicurezza informatico ed eventualmente di un data breach, il gruppo verrà convocato e 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 deve essere coinvolto il Responsabile della Protezione dei Dati (RPD) designato, 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 soggetto esterno cui è affidato il Servizio ICT per l'Ente ha il compito di individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del RPD, e di segnalare al personale competente le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali.

Il personale appositamente individuato dovrà coinvolgere, a seconda della gravità dell'incidente, i vertici dell'Ente o i diversi Responsabili competenti per gli aspetti di comunicazione interna ed esterna e nel caso, durante la gestione dell'incidente, emergano responsabilità da parte di personale interno dell'Ente occorre coinvolgere la struttura che si occupa di 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 personale individuato deve valutare l'opportunità o la necessità, di coinvolgere le strutture di riferimento regionali e nazionali (ad esempio LepidaSpA considerando il proprio ruolo nell'ambito della sicurezza della Community Network, CERT-PA, ...). Inoltre, il personale addetto deve prevedere il coinvolgimento dei fornitori dell'Ente di servizi ICT per il supporto all'analisi e per l'ottenimento di informazioni utili oltre alle autorità di pubblica sicurezza nel caso in cui l'incidente possa presentare risvolti dal punto di vista penale.

In caso di data breach il punto di contatto con il Garante per la protezione dei dati personali è costituito dal Responsabile Protezione dei dati (RPD).

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 dall'Ente per mettere in sicurezza i sistemi ICT.

PROCEDURA DI GESTIONE DEGLI INCIDENTI DI SICUREZZA

Deve essere sviluppata, documentata e tenuta aggiornata una procedura per la gestione degli incidenti di sicurezza. Tale procedura ha i seguenti obiettivi:

- 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 della Sicurezza ICT con l'eventuale supporto delle figure ritenute necessarie tenendo conto della complessità e variabilità dell'argomento trattato.

Per facilitare la gestione degli incidenti di sicurezza occorre mantenere operativo un workflow che automatizzi le varie fasi, in particolare il flusso delle comunicazioni fra i vari attori. Tale

misura ha anche lo scopo di facilitare la produzione del report relativo all'incidente e di tenere aggiornate le statistiche sugli incidenti di sicurezza.

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 occorrerà intraprendere tutte le operazioni necessarie a garantire la continuità operativa dell'Ente.

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 di sicurezza, comprensiva delle evidenze e delle valutazioni effettuate, viene elaborata in maniera tale da non indicare dati personali. Il tempo di conservazione di tale documentazione è stabilito in 24 mesi nel caso in cui siano presenti dati personali, allo spirare del quale i dati devono essere cancellati e senza limiti di tempo nel caso non siano presenti dati personali.

Tutti i dipendenti e collaboratori dell'Ente che accedono alle risorse del Sistema Informatico Informativo dell'Ente 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.

DETTAGLI DELLA PROCEDURA DI GESTIONE DEGLI INCIDENTI DI SICUREZZA

PREPARAZIONE

Si tratta di attività necessarie per consentire una adeguata gestione degli incidenti informatici di sicurezza. 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.

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.

GESTIONE DEL DATA BREACH

1. Data Breach Interno

Ogni incaricato autorizzato a trattare dati personali, qualora venga a conoscenza di un potenziale caso di data breach, avvisa tempestivamente il soggetto interno dell'Area Tecnica o Urbanistica appositamente individuato per la gestione degli incidenti di sicurezza.

Questi soggetti incaricati valutano l'evento, avvalendosi di eventuali altre professionalità necessarie per la corretta analisi della situazione e del RPD, e se confermano le valutazioni di potenziale data breach con conseguente rischio per i diritti e le libertà delle persone fisiche, procedono con la convocazione del Gruppo per la Gestione della Sicurezza ICT.

2. Data Breach Esterno

Ogni Responsabile esterno del trattamento, qualora venga a conoscenza di un potenziale caso di data breach che riguarda dati personali cui il Comune di Sestola sia titolare e di cui è tenuto ad effettuare il trattamento in forza di convenzioni o contratti, ne dà avviso senza giustificato ritardo al Comune stesso, inviando una mail agli incaricati individuati nell'Area Tecnica e Urbanistica (ambiente@comune.sestola.mo.it urbanistica@comune.sestola.mo.it). La notizia dovrà pervenire, comunque, al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del Responsabile esterno.

Questi soggetti incaricati valutano l'evento, avvalendosi di eventuali altre professionalità necessarie per la corretta analisi della situazione e del RPD, e se confermano le valutazioni di potenziale data breach con conseguente rischio per i diritti e le libertà delle persone fisiche, procedono con la convocazione del Gruppo per la Gestione della Sicurezza ICT.

Le segnalazioni di incidente di sicurezza può arrivare in modo automatico da strumenti appositi o da un processo di analisi continuativa degli eventi di sicurezza registrati da vari dispositivi o anche direttamente da parte di un utente, il quale può per esempio rilevare situazioni di alterazioni di un sito web dell'Ente, di accesso non autorizzato a dati, di indisponibilità di una risorsa ICT per un tempo prolungato, ecc.... Le segnalazioni degli utenti sono inoltrate ai soggetti incaricati dell'Area Tecnica e Urbanistica per essere sottoposte ad una analisi preliminare prima del coinvolgimento eventuale del Gruppo per la Gestione della Sicurezza ICT.

Nel caso di segnalazioni di incidente da parte di soggetti terzi, l'Ente avvia senza indugio un'indagine volta a verificare che sia avvenuta effettivamente la violazione di dati segnalata. La notifica viene effettuata al Garante qualora gli esiti della breve e spedita indagine consentano di appurare l'effettiva verifica della violazione (quindi solo al termine dell'indagine).

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 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.
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.: black out, incendio, allagamento, terremoto) in grado di condizionare direttamente l'operatività dei sistemi informatici.

E' 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 per la Gestione della Sicurezza ICT deve anche stabilire la gravità dell'incidente di sicurezza, per fare ciò può inizialmente avvalersi della seguente tabella contraddistinta da una valutazione di tipo qualitativo, ma la classificazione della gravità dell'incidente è comunque a totale discrezione del Gruppo stesso.

Gravità incidente di sicurezza	Descrizione
Alta	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.

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 offerti dall'ente con conseguente perdita di produttività da parte degli utilizzatori; • 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 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 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.

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 effettuasse 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 dovranno essere informati tempestivamente tutti gli ulteriori soggetti coinvolti nell'episodio.

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 trattati.

In caso di data breach l'Ente 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” e 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.

In caso di data breach deve essere sempre coinvolto il Responsabile Protezione Dati (RPD) per la valutazione dei rischi per i diritti e le libertà delle persone fisiche, il quale esprime anche formale parere sulla necessità di effettuare notifiche.

COMUNICAZIONE DEGLI INCIDENTI

Tutti i potenziali incidenti dovranno essere comunicati come primo punto di contatto Al personale appositamente incaricato dell'Ente adibito alla gestione della sicurezza via mail, o attraverso specifiche modalità adottate dall'Ente..

La notifica della violazione al Garante

Nei casi in cui l'incidente consista in una violazione di dati personali, l'Ente deve notificare l'incidente al Garante per la protezione dei dati personali se, sulla scorta della valutazione approfondita, strutturata e documentata di cui al paragrafo precedente, si assuma come probabile che la violazione dei dati personali presenti effettivamente un rischio per i diritti e le libertà delle persone fisiche.

La comunicazione al Garante deve essere redatta dai soggetti tenuti nell'adempire all'obbligo previsto dall'art. 33 del Regolamento UE nr. 679/2016 e dall'art. 26 del d.lgs. nr. 51/2018, in aderenza allo specifico modello predisposto dall'Autorità con le modalità di cui all'art. 65 del d.lgs. 82/2005, mediante i sistemi telematici indicati nel sito istituzionale del garante.

La notifica 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' art. 34 del Regolamento UE nr. 679/2016, 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 Responsabile Protezione Dati (RPD);
- 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.

Nel caso in cui il numero di interessati lo consenta, la comunicazione deve essere inviata a mezzo mail (o pec) e con avviso pubblicato sul sito istituzionale nel caso in cui il numero di soggetti coinvolti sia particolarmente ingente.

ATTIVAZIONE DELLA PROCEDURA E MONITORAGGIO DELLE ATTIVITÀ

L'attivazione della procedura di gestione incidenti, mediante le opportune segnalazioni nel workflow sarà a carico del personale dell'Area Tecnica e Urbanistica appositamente incaricato, il quale, a seconda della gravità attribuita in fase di identificazione dell'incidente, attiverà il Gruppo per la Gestione della Sicurezza ICT e informerà il RPD.

Per ogni incidente di sicurezza il personale addetto redige un Rapporto, documento dinamico da aggiornare in ogni fase della gestione dell'incidente, inserendo soltanto le parti che nelle rispettive fasi è possibile conoscere e che sarà poi completato in tutte le parti in fase di chiusura dell'incidente.

Il rapporto deve essere conservato per la durata di 5 anni, in formato elettronico, in una

cartella soggetta a backup periodico e ad accesso opportunamente limitato.

E' fondamentale che tutte le operazioni eseguite per la gestione di un eventuale incidente siano opportunamente tracciate, permettendo in tal modo di poter identificare tutti i soggetti coinvolti nelle operazioni tecniche di gestione e poterli 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.

CONTENIMENTO, RIMOZIONE E RIPRISTINO

Le operazioni di contenimento hanno due importanti fini:

- evitare che il danno si propaghi od almeno limitarne la diffusione;
- acquisire le eventuali evidenze digitali di reato prima che queste possano essere compromesse.

Quest'ultima attività è molto critica, infatti, è necessario:

- 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;
- le attività di contenimento dovranno essere eseguite da personale qualificato, ovvero da sistemisti o esperti applicativi appositamente addestrati per eseguire le operazioni necessarie.

Tutte le operazioni eseguite saranno comunque sotto la responsabilità del personale appositamente individuato per la sicurezza informatica 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.

Tali soggetti avranno anche il compito di comunicare al Titolare del trattamento quanto eseguito al termine di questa fase.

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

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.

E' 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 dell'Ente;
- interruzione di pubblici servizi critici;
- violazioni della privacy di utenti e cittadini;
- 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. 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.

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 temporaneamente sino a quando non sia possibile procedere con le operazioni di rimozione definitiva di quanto ha scatenato l'incidente.

Durante questa fase, possono emergere diverse necessità, 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 altri Servizi/Direzioni dell'Ente per comunicare eventuali disservizi. In tali casi il personale addetto alla sicurezza informatica può operare le corrette scelte in collaborazione col Gruppo di Gestione della Sicurezza ICT e comunicherà al Titolare del trattamento le eventuali azioni che saranno intraprese.

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 per la Gestione della Sicurezza ICT, eventualmente coinvolgendo tutti i soggetti interessati e fornendo al Titolare del trattamento, tramite un report di dettaglio, le indicazioni degli eventuali costi da sostenere e 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.

RIPRISTINO

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.

E' 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.

ATTIVITA' POST- INCIDENTE

La decisione del momento in cui un sistema coinvolto in un incidente possa ritornare in produzione è in carico al Gruppo per la Gestione della Sicurezza ICT che, definisce un piano di riattivazione dei diversi servizi impattati dall'incidente, di cui informa il Titolare del trattamento.

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 Gruppo per la Gestione della Sicurezza ICT 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.

Sono documentati e archiviati, in modalità distinguibile rispetto agli incidenti di sicurezza, tutti i data breach, seppure non notificati 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 Rapporto relativo all'incidente stesso da parte del personale addetto e incaricato della Sicurezza informatica.

Il Rapporto, firmato digitalmente dal personale appositamente incaricato della Sicurezza tramite procedura di hashing a garanzia della sua integrità, dovrà essere consegnato al Gruppo per la Gestione della Sicurezza ICT e dovrà essere inviato in forma riservata sotto forma di relazione sull'esito dell'incidente di sicurezza al Titolare del trattamento .

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).

E' fondamentale che i punti critici rilevati durante l'esecuzione delle operazioni siano immediatamente condivisi con i componenti del team di gestione degli incidenti 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 agendo sulle infrastrutture e i sistemi.

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? E' risultata adeguata al contesto?
- Si sono presentati aspetti che hanno rallentato la risoluzione dell'incidente?
- Si sono presentati elementi che si ritiene siano da cambiare in modo da rendere il processo di gestione degli incidenti più efficace ed efficiente?
- E' 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?
- E' necessario modificare le policy aziendali dal punto di vista tecnico (es.: aggiungere file con una determinata estensione tra quelli bloccati dal sistema antivirus)?
- E' 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 aggiuntive (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 anti-intrusione 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 scaturiscono debbano divenire patrimonio comune all'interno del team di gestione degli incidenti.

Per questo motivo occorre che entro breve termine dalla chiusura formale di un incidente, il Gruppo per la Gestione della Sicurezza ICT 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 nel Rapporto le considerazioni e le operazioni che possono portare a migliorare l'intera procedura.

