ASP "Cav. Marco Rossi Sidoli"
Via Duca degli Abruzzi n. 27 -43053- Compiano (PR)
Tel. 0525-825116 Fax 0525-825374 E-mail info@rossisidoli.com
P. IVA 00799990346 - C. F. 81000140343

Policy gestione incidenti di sicurezza

Allegato A delibera del CdA n. 57 del 22/10/2018

Sommario

1. Premessa

Il presente documento rappresenta il riferimento dell'Azienda Pubblica di Servizi alla Persona (ASP) "Cav. Marco Rossi Sidoli" per la regolamentazione della gestione degli incidenti di sicurezza informatica che possano occorrere ai servizi e 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 GDPR n. 679/2016, il presente documento individua quali siano le violazioni che ricadono nell'ambito della suddetta normativa, i casi in cui ASP debba notificare i *data breach* all'Autorità Garante e agli interessati, le misure atte a trattare il rischio e la documentazione da produrre.
Si rappresenta che l'art. 32 del suddetto GDPR n. 679/2016 (di seguito Regolamento) 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'Azienda.
L'ambito di applicazione è rappresentato da sistemi ICT di ASP e vengono presi in considerazione incidenti che possano scaturire sia dall'azione di un attacco informatico portato da elementi esterni all'organizzazione, sia da un eventuale comportamento negligente o scorretto, di natura ostile con obiettivi frodatori da parte di uno o più collaboratori dell'Azienda.
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).
Il presente documento è applicabile alle risorse e ai servizi di tipo informatico gestiti in modo diretto oppure esternalizzato da parte di ASP "Cav. Marco Rossi Sidoli".

2. 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, correlate a 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.

3. Data breach ai sensi del GDPR

Il Regolamento 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 propri diritti, la discriminazione, il furto d'identità o la frode, la perdita finanziaria, l'inversione non autorizzata di pseudonimizzazione, il danno alla reputazione e la perdita di riservatezza dei dati personali protetti dal segreto professionale. Può anche includere qualsiasi altro significativo svantaggio economico o sociale per gli individui che ne siano oggetto.

4. Notifica al Garante e agli interessati

In caso di *data breach* ASP valuta 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'Azienda effettua la notifica al Garante delle violazioni di dati personali.
Quando le violazioni di dati comportino un rischio valutato come elevato per i diritti e le libertà delle persone fisiche, 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.
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;
- le 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 viene condotta secondo una metodologia operativa adeguata, di seguito dettagliata.

ASP notifica la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui la medesima è stata rilevata.

Oltre tale termine, tale notifica è corredata delle ragioni del ritardo e le informazioni sono fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il termine decorre dal momento in cui l'Azienda ha consapevolezza della violazione di dati, ovverosia quando raggiunge un ragionevole grado di certezza che si è verificato un incidente di sicurezza che ha compromesso i dati personali dalla stessa trattati.
ASP può tardare la notifica all'Autorità Garante nei casi in cui la medesima possa produrre effetti negativi sugli individui interessati.
Nei casi in cui l'Azienda disponga di informazioni solo parziali della violazione, effettua comunque 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.
ASP utilizza lo strumento più efficace affinché tale comunicazione sortisca il maggiore effetto possibile.

5. 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 e in grado di prendere rapidamente le decisioni imposte dalla delicatezza del compito assegnato.

ASP istituisce a tal fine un **Gruppo per la Gestione della Sicurezza ICT**, adeguatamente dimensionato e strutturato con 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 aziendali, provvedendo che il medesimo sia sempre aggiornato.

Il **Gruppo per la Gestione della Sicurezza ICT** è costituito dalle seguenti figure:

- Direttore con il ruolo di **Responsabile per la gestione della sicurezza ICT;**
- Responsabile del Servizio Affari Generali con il ruolo di **Referente per la gestione della sicurezza informatica**;

I riferimenti del **Gruppo per la Gestione della Sicurezza ICT** (nominativi, indirizzo e-mail, numero di telefono ecc.) sono pubblicati sul sito istituzionale dell'Azienda nella sezione di Amministrazione trasparente "organizzazione/telefono e posta elettronica".

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 Responsabile cui fa capo il Servizio e/o la struttura i cui dati sono stati oggetto di *data breach* e da tutti coloro che il Gruppo stesso riterrà necessario coinvolgere, a seconda della tipologia di incidente e della tipologia di dati coinvolti.

Nelle attività del Gruppo deve essere coinvolto il *Data Protection Officer* (DPO) 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 **Responsabile per la gestione della sicurezza ICT** ha il compito di attivare il Gruppo in caso di incidenti di sicurezza, di individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO, e di segnalare al Titolare, in persona del Legale Rappresentante pro tempore, 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 Responsabile deve inoltre coinvolgere, a seconda della gravità dell'incidente, il Consiglio di Amministrazione e i Responsabili di Servizio dell'Azienda per gli aspetti di comunicazione interna ed esterna e, nel caso in cui, durante la gestione dell'incidente, emergano responsabilità da parte di personale interno, per gli eventuali provvedimenti disciplinari di competenza.

Nel caso in cui le attività di analisi dell'incidente di sicurezza evidenzino particolari difficoltà oppure impatti che si estendano al di fuori del perimetro aziendale, il Responsabile deve valutare l'opportunità o la necessità, di coinvolgere le strutture di riferimento regionali e nazionali (ad esempio, Lepida SpA, considerando il proprio ruolo nell'ambito della sicurezza della Community Network, CERT-PA, …). Inoltre, il Responsabile, oltre a coinvolgere i propri fornitori di servizi ICT per il supporto all'analisi e per l'ottenimento di informazioni utili, deve prevedere anche il coinvolgimento delle 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 *Data protection officer*.

Il **Referente per la gestione della sicurezza informatica** è la figura che deve farsi carico della gestione di eventuali incidenti e cura che siano attivati comportamenti, attività e regolamenti per cercare di prevenire gli incidenti di sicurezza, riducendo il livello di rischio e l'esposizione a possibili attacchi informatici.

6. Procedura di gestione degli incidenti di sicurezza

ASP di seguito definisce la procedura per la gestione degli incidenti di sicurezza e ne garantisce il necessario aggiornamento..
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 sicurezza 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. 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 in un piano di continuità operativa dell'Ente adottato 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 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 di ASP 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'Azienda, 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.

6.1 Identificazione e analisi dell'incidente

Tutti i potenziali incidenti di sicurezza di cui i dipendenti aziendali (utenti interni) siano a conoscenza, devono essere dagli stessi immediatamente comunicati, come primo punto di contatto, al Servizio Pianificazione e Controllo, la struttura organizzativa aziendale adibita alla gestione della sicurezza ICT.

Le segnalazioni di possibili incidenti di sicurezza devono pervenire via mail al **Referente per la gestione della sicurezza informatica**.

Le segnalazioni possono arrivare al Referente, anche da alert automatici del sistema informativo aziendale, o da parte di utenti che, per esempio, possono rilevare situazioni di alterazione del sito web aziendale, di accesso non autorizzato a dati, di indisponibilità di una risorsa ICT per un tempo prolungato etc.

Nel caso di riscontro positivo di una segnalazione che pervenga in modo automatico dal processo di analisi continuativa degli eventi di sicurezza registrati da vari dispositivi, viene aperto un incidente di sicurezza che segue la procedura di gestione.

Nel caso di segnalazioni di incidente da parte di soggetti terzi, il Referente si attiva immediatamente per valutare se l'evento segnalato sia effettivamente riconducibile a un incidente di sicurezza, oppure si tratti di un cosiddetto falso positivo.

La notifica prevista dall'art. 33 del Regolamento viene effettuata al Garante a conclusione della verifica, qualora gli esiti della stessa consentano di appurare l'effettiva sussistenza della violazione.

a. VALUTAZIONE DELL'IMPATTO DELL'INCIDENTE

I possibili reali incidenti di sicurezza si possono classificare in diverse tipologie, dettagliate 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

Il **Referente**, a seguito della verifica della sussistenza di un reale incidente, effettua 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 ai seguenti parametri:

- il livello di criticità della risorsa ICT coinvolta, determinato in base alle valutazioni inerenti 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 Referente della sicurezza informatica del gruppo sicurezza ICT, anche coinvolgendo il referente della società incaricata della progettazione e della tenuta del sistema informatico aziendale e i tecnici informatici a disposizione dell'Azienda, deve anche stabilire la **gravità** dell'incidente di sicurezza. Per fare ciò può inizialmente avvalersi della seguente matrice contraddistinta da una valutazione di tipo qualitativo, ma la classificazione della gravità dell'incidente è comunque a sua totale discrezione.

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'Azienda ● 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 minuti ei 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.

Poiché per alcuni incidenti può risultare difficile assegnare un livello di gravità definitivo prima che l'analisi sia completa, occorre che la valutazione sia effettuata sulla base delle evidenze note sino a quel momento, assumendo che la gravità potrebbe molto probabilmente aumentare nel caso in cui non si effettui alcuna operazione di contenimento.
Il Referente, verificare comunque ciclicamente, nel periodo in cui l'incidente è in corso, la gravità assegnata allo stesso, in quanto essa può variare nel tempo.
Effettuata una prima analisi, ancorché non definitivamente conclusa, il Referente informa tempestivamente il **Responsabile per la gestione della sicurezza ICT,** che provvede ad attivare il **Gruppo per la Gestione della Sicurezza,** deputato alla gestione incidenti e, in caso di *data breach*, informa immediatamente il DPO, e il Legale Rappresentante dell'Azienda. Nel contempo, il **Referente,** sulla base della gravità appurata dell'incidente, **attiva direttamente** la **procedura di gestione incidenti,** secondo quanto più dettagliatamente descritto al successivo punto D)..

B. VALUTAZIONE DEI RISCHI DERIVANTI DAL VERIFICARSI DEL DATA BREACH

In caso di *data breach* il Gruppo per la gestione della Sicurezza ICT valuta 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 così come declinata nel precedente paragrafo 3;
- 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 minorenni 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 a 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* il Data Protection Officer (DPO) è sempre coinvolto nella valutazione dei rischi per i diritti e le libertà delle persone fisiche ed esprime anche formale parere sulla necessità di effettuare la notifica.

C. COMUNICAZIONE DEGLI INCIDENTI

La notifica della violazione al Garante

Nei casi in cui l'incidente consista in una violazione di dati personali, il Titolare, nella persona del Legale Rappresentante pro tempore, 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, da redigere sulla base del modello allegato al presente documento quale parte integrante e sostanziale (all.1), deve ricomprendere ogni informazione utile, oltre che la descrizione:

- della natura della violazione dei dati personali;
- delle categorie e del numero approssimativo di interessati in questione, nonché delle categorie e del numero approssimativo di registrazioni dei dati personali in questione;
- delle probabili conseguenze della violazione dei dati personali;
- delle 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;
- i recapiti del Data Protection Officer.

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'allegato 1 del presente documento, deve essere formulata con linguaggio chiaro e comprensibile agli utenti e 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.

Nel caso in cui il numero di interessati lo consenta, la comunicazione deve essere inviata a mezzo mail (o pec, o sms) e comunque con avviso pubblicato sul sito istituzionale. Nel caso in cui il numero di soggetti coinvolti sia particolarmente ingente, è sufficiente effettuare la comunicazione dell'avvenuta violazione di dati utilizzando il sito istituzionale.

D. ATTIVAZIONE DELLA PROCEDURA E MONITORAGGIO DELLE ATTIVITÀ

L'attivazione della procedura di gestione incidenti, è a carico del **Referente per la gestione della sicurezza informatica**, il quale, a seconda della gravità attribuita in fase di identificazione dell'incidente, utilizzerà diverse modalità di attivazione e tracking.

Incidente di gravità "Alta"

Il Referente per la gestione della sicurezza informatica informa immediatamente il **Responsabile della Sicurezza** per il coinvolgimento del gruppo Gestione Sicurezza mediante l'invio dell'apposito Rapporto incidente di sicurezza, compilando soltanto le parti che in questa fase è possibile conoscere.

Lo scopo principale di questa prima fase è di attivare il gruppo sicurezza per la gestione dell'incidente ed eventualmente anche informare il DPO nel caso di un data breach. Il Rapporto incidente di sicurezza sarà poi completato in tutte le sue parti in fase di chiusura dell'incidente.

Il Responsabile della Sicurezza, deve conservare per la durata di cinque anni il Rapporto, in formato elettronico, in una cartella soggetta a backup periodico e ad accesso opportunamente limitato.

E' 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 formano quindi una base dati che andrà ad incrementare la conoscenza dell'Azienda in merito agli incidenti di sicurezza informatica.

Nel caso in cui l'incidente di sicurezza abbia un impatto sulla continuità operativa per un tempo di disservizio inaccettabile per gli utenti interni ed esterni (superiore al RTO dichiarato in sede di BIA), è necessario attivare il Gruppo sicurezza

Incidente di gravità "Media" o "Bassa"

In caso di incidente di gravità media o bassa, l'incidente può essere completamente gestito dal referente per la gestione della sicurezza informatica fermo restando il coinvolgimento del Responsabile della Sicurezza e, nel caso di un data breach, del DPO. In tale caso non è necessaria (anche se è consigliabile) la stesura del Rapporto di Incidente di Sicurezza, ma è comunque necessario tracciare opportunamente le operazioni permettendo in tal modo di poter identificare tutte le risorse coinvolte nelle operazioni tecniche di gestione e di poterle eventualmente indicare in ambito giudiziale come testimoni.

Anche in questo caso le indagini svolte e le operazioni di gestione formano una base dati che andrà a incrementare la conoscenza dell'Azienda in merito agli incidenti di sicurezza informatica.

I dati raccolti saranno resi disponibili, attraverso diversi profili di consultazione, anche a fini statistici, al Responsabile della Sicurezza, ai membri del gruppo sicurezza e al Legale Rappresentante dell'Azienda

6.2 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.

A tal fine 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, dipendenti dell'Azienda o dalla medesima incaricati.
Tutte le operazioni eseguite saranno comunque sotto la responsabilità del Referente per la sicurezza informatica il quale dovrà riportare nel Rapporto di incidente:

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

Il Referente per la sicurezza informatica dovrà comunicare al Responsabile della sicurezza quanto eseguito al termine di questa fase, raccordandosi poi con il Responsabile del Servizio Affari
Generali e Giuridico Legali per la trasmissione di copia della documentazione utile ai fini della proposizione delle azioni legali di competenza.
Le operazioni di contenimento possono essere di due tipologie: a breve termine e a lungo termine.

A. 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, non esaustivi, 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 preveda un prosieguo in ambito legale come per esempio:

- accessi abusivi a sistemi o informazioni;
- attività illecite commesse da dipendenti o da utenti dei servizi aziendali comunque mediante il sistema informativo gestito dell'Azienda;
- interruzione di pubblici servizi critici;
- violazioni della privacy di dipendenti, 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 e i programmi utilizzati per effettuare le comuni operazioni di backup e hanno lo scopo di mettere in sicurezza le informazioni necessarie per un' eventuale reinstallazione del dispositivo.

B. 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 a operazioni più complesse di rimozione delle cause.

A titolo esemplificativo e non esaustivo, si possono indicare quali operazioni di contenimento a lungo termine:

- 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 le Aree/Servizi dell'Azienda per comunicare eventuali disservizi.

In tali casi il Referente per la sicurezza informatica può operare le corrette scelte in autonomia, comunicando al Responsabile della Sicurezza le eventuali azioni che saranno intraprese e raccordandosi, secondo quanto precedentemente indicato, con il Responsabile del Servizio Affari Generali e Giuridico Legali.

C. 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 a 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, ad esempio, 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.

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 Responsabile della sicurezza, tramite un report di dettaglio, le indicazioni degli eventuali costi da sostenere e dei tempi necessari al ripristino, affinché il medesimo possa informare il Legale rappresentante e il Consiglio di Amministrazione.

Poiché l'operazione di contenimento a lungo termine non è da considerarsi risolutiva del problema, ma solo ed esclusivamente un'azione a titolo temporaneo, l' Azienda si impegna a contenere i tempi necessari per poter procedere alla fase di rimozione ai tempi tecnici strettamente necessari alla definizione dell'intervento, al reperimento delle relative risorse economiche e alle operazioni di approvvigionamento.

D. 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.

6.3 Attività post-incidente

La decisione del momento in cui un sistema coinvolto in un incidente possa ritornare in produzione è in carico al Referente per la sicurezza informatica che, in collaborazione con il Gruppo per la gestione della sicurezza ed eventuali gruppi di supporto tecnici coinvolti, 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 monitoraggio 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 ai restanti 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 report relativo all'incidente stesso da parte del Referente per la sicurezza informatica.

Il report, firmato digitalmente dal Responsabile della Sicurezza, 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 Legale Rappresentante, al Consiglio di Amministrazione e ai Dirigenti responsabili dei Servizi coinvolti.

Il Responsabile della Sicurezza deve conservare il Rapporto in un repository ad accesso limitato ai membri del proprio staff, per cinque anni o per tutto il tempo ritenuto necessario (ad esempio allo svolgimento di indagini, nel caso di conseguenze penali, o perlomeno alla definitiva rimozione delle cause scatenanti l'incidente).

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' Azienda (consultabile ad accesso ristretto in base al ruolo ricoperto nel processo di gestione incidenti).

I punti critici rilevati durante l'esecuzione delle operazioni saranno condivisi con i componenti del team di gestione degli incidenti e si provvederà nel più breve tempo possibile a predisporre quanto 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.

Per la rilevazione di eventuali criticità il Gruppo di gestione della sicurezza, eventualmente allargato a figure che siano state parte attiva nella gestione dell'incidente, verificherà tramite apposita checklist se:

- la procedura di gestione incidenti sia stata correttamente eseguita;
- la procedura sia risultata adeguata al contesto;
- si siano presentati aspetti che abbiano rallentato la risoluzione dell'incidente;
- si siano presentati elementi che si ritiene debbano essere cambiati in modo da rendere il processo di gestione degli incidenti più efficace ed efficiente;
- sia necessario aggiornare il metodo di analisi della gravità a valle dell'incidente;
- siano necessarie delle azioni correttive da intraprendere in fase di mitigazione dei rischi onde evitare che l'incidente possa riaccadere;
- sia necessario modificare le policy aziendali dal punto di vista tecnico (es.: aggiungere file con una determinata estensione tra quelli bloccati dal sistema antivirus;
- sia 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;
- siano necessarie risorse addizionali (es.: personale, tools, strumenti hardware o software) per rendere il processo di gestione degli incidenti più efficace ed efficiente;
- siano 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);

Scopo di tale operazione è quello di verificare che il processo di gestione incidenti sia risultato adeguato a fronteggiare la situazione e far si che le considerazioni che ne scaturiscono diventino patrimonio comune all'interno del team di gestione degli incidenti.
Per questo motivo, entro breve termine dalla chiusura formale di un incidente, il Responsabile della Sicurezza convoca il Gruppo per la gestione della sicurezza e le eventuali figure che sono state parte attiva nella gestione dell'incidente, con l'obiettivo di valutare collegialmente l'efficacia della procedura di gestione degli incidenti e definire in un apposito verbale le considerazioni e le operazioni che possano portare a migliorare l'intera procedura.

Allegato 1

Rapporto incidente di sicurezza

1. Premessa:
(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.).

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);
(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).

Compiano , li …….

Responsabile della Sicurezza
(nome e cognome)