Versione: 7.3
Autore: Giannandrea (4/11/2020)
Modificato: Simone Giovanardi (21/04/2022)
Verificato: Tutti i Direttori (28/04/2022)
Approvato: Mazzini (02/05/2022)
Classificazione: uso esterno

PROCEDURA PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA

1. Scopo e campo di applicazione

Il presente documento rappresenta per Lepida ScpA il riferimento per la gestione degli incidenti di sicurezza che possono coinvolgere le attività operative dell'organizzazione, i servizi erogati e le informazioni trattate. Gli incidenti possono essere causati da eventi sia intenzionali sia accidentali e possono avere origine sia interna sia esterna all'organizzazione.
Ogni organizzazione deve necessariamente attuare una serie di misure di natura sia tecnica sia organizzativa per cercare di prevenire gli incidenti di sicurezza. Tuttavia una volta che l'incidente si verifica è necessario gestirlo in modo corretto e tempestivo al fine di annullarne o minimizzarne l'impatto. Attraverso l'analisi e la comprensione dei meccanismi tramite cui gli incidenti si verificano e delle modalità utilizzate per la loro gestione, è inoltre possibile migliorare continuamente la capacità di risposta.
L'ambito di applicazione del presente documento è rappresentato da tutte le risorse, i servizi tecnologici e le informazioni, sia in formato elettronico sia in altra forma (es. documenti cartacei, comunicazioni orali), gestiti autonomamente da Lepida ScpA o affidati ad essa da soggetti esterni (es. clienti, utenti). Sono tenuti a conoscere e ad applicare quanto riportato nel presente documento sia i dipendenti di Lepida ScpA sia, nei limiti delle responsabilità e delle modalità operative definite a livello contrattuale, i collaboratori, i fornitori e gli ulteriori soggetti esterni che possono essere coinvolti nella gestione di incidenti di sicurezza o che effettuano trattamenti di dati personali per conto di Lepida ScpA.
Il presente documento individua inoltre:

- le violazioni di dati personali che richiedono notifica al Garante per la protezione dei dati personali e agli interessati, secondo quanto previsto dal Regolamento UE (GDPR) 679/2016 (Artt. 33 e 34);
- le violazioni al servizio di Identity Provider SPID (Sistema Pubblico di Identità Digitale) che richiedono notifica all'Agenzia per l'Italia Digitale (AgID) ed eventualmente al Garante per la protezione dei dati personali e agli interessati come previsto dal "Regolamento recante le modalità attuative per la realizzazione dello SPID" (Artt. 30 e 30 bis).

Il processo adottato da Lepida ScpA per la gestione degli incidenti di sicurezza delle informazioni segue le buone pratiche definite nelle norme ISO/IEC 27002 e ISO/IEC 27035 e le raccomandazioni NIST SP 800-61 rev. 2.

2. Definizioni

Nel presente documento si applicano le seguenti definizioni:

- Incidente di sicurezza: evento indesiderato o imprevisto che ha una significativa probabilità di compromettere la disponibilità di un servizio dell'organizzazione e/o la disponibilità, la riservatezza o l'integrità delle informazioni trattate in qualsiasi forma esse siano (es. formato digitale, documento cartaceo);
- Violazione di dati personali (o data breach): incidente di sicurezza che comporta accidentalmente o in modo illecito:
    - la perdita dell'accesso a o la distruzione dei dati personali trattati (violazione di disponibilità);
    - la modifica dei dati personali trattati (violazione di integrità);
    - l'accesso a o la divulgazione non autorizzata dei dati personali trattati (violazione di riservatezza).

3. Ruoli e responsabilità interne all'organizzazione

Il Direttore Generale, i Direttori/Vicedirettori di Divisione e i Coordinatori di Aggregato hanno le seguenti responsabilità:

- assicurare la disponibilità di risorse e competenze adeguate per la gestione degli incidenti;
- assicurare l'esecuzione periodica delle valutazioni dei rischi per la sicurezza delle informazioni;
- assicurare l'applicazione delle misure di prevenzione stabilite;
- assicurare la tempestività e l'efficacia della risposta agli incidenti rilevati;
- assicurare le attività di notifica degli incidenti verso i soggetti esterni interessati;
- assicurare la documentazione degli incidenti occorsi;
- assicurare il riesame degli incidenti occorsi al fine di migliorare le misure di sicurezza applicate e il processo di gestione degli incidenti.

Essi compongono anche il **Comitato di crisi** che, in situazioni di emergenza, assume le seguenti responsabilità:

- valutazione delle situazioni di disastro e dichiarazione dello stato di emergenza;
- coordinamento e supervisione di tutte le operazioni e decisioni per affrontare l'emergenza, ridurne l'impatto e ripristinare le condizioni preesistenti;
- valutazione della necessità di effettuare comunicazioni e definizione dei contenuti e delle modalità;
- cessazione dello stato di emergenza.

Da un punto di vista operativo le Aree aziendali competenti per le attività di risposta agli incidenti e ripristino, e i relativi ambiti di intervento, sono riportate nella tabella seguente.

AMBITO	**AREE AZIENDALI**
Postazioni di lavoro e dispositivi per utenti	Servizi IT e Sistemi Periferici (Divisione Datacenter & Cloud)
Sistemi informatici, infrastrutture IT, reti e servizi di data center	Attivazioni & Esercizio DC & Cloud (Divisione Datacenter & Cloud)
Facility di data center	Realizzazione & Manutenzione DC & Cloud (Divisione Datacenter & Cloud)
Apparati e servizi delle reti Lepida, ERretre e ERWiFi	Attivazioni & Esercizio Reti (Divisione Reti)
Infrastrutture e facility delle reti Lepida, ERretre e ERWiFi	Realizzazione & Manutenzione Reti (Divisione Reti)
Software applicativi	Interoperabilità & Manutenzione Piattaforme e Servizi (Divisione Software & Piattaforme Enti & Sanità)
Servizi di piattaforme digitali	Attivazioni & Esercizio Piattaforme e Servizi (Divisione Software & Piattaforme Enti & Sanità), Interoperabilità & Manutenzione Piattaforme e Servizi (Divisione Software & Piattaforme Enti & Sanità)

Servizi di welfare digitale	Attivazioni & Esercizio Welfare (Divisione Welfare Digitale)
Archivi e servizi di digitalizzazione	Digitalizzazione & Dematerializzazione (Divisione Integrazioni Digitali)
Servizi di amministrazione digitale	Amministrazioni Digitali ((Divisione Integrazioni Digitali)
Servizi di accesso	Supporto ai Contatti e all'Accesso (Divisione Accesso)
Altro	Tutte le Aree Divisionali aziendali in base alla competenza

TABELLA 1

Lepida ScpA ha inoltre designato un Responsabile della Protezione dei Dati (RPD), che deve essere coinvolto per acquisirne il parere in relazione all'adeguatezza delle misure di sicurezza applicate o da applicare e, in caso di data breach, in ordine alla necessità di effettuare la notifica al Garante per la protezione dei dati personali ed eventualmente agli interessati, e costituisce il punto di contatto dell'organizzazione verso il Garante.

4. Procedura di gestione degli incidenti di sicurezza

La procedura di gestione degli incidenti adottata da Lepida ScpA è strutturata nelle seguenti fasi, descritte di seguito in dettaglio:

- Preparazione;
- Rilevazione e analisi;
- Contenimento e acquisizione di evidenze digitali di reato;
- Rimozione e ripristino;
- Notifiche;
- Attività post-incidente.

4.1 Preparazione

La preparazione consiste nell'insieme di attività attraverso le quali l'organizzazione cerca di prevenire gli incidenti e si organizza per essere in grado di gestirli efficacemente quando si verificano.
Fra le attività previste si possono citare le seguenti:

- predisporre le liste di contatto dei soggetti (es. dipendenti, collaboratori, fornitori, clienti, altri soggetti esterni) che possono essere coinvolti nella gestione degli incidenti;
- predisporre i canali di comunicazione per la segnalazione degli incidenti;
- predisporre un sistema di trouble ticketing;
- predisporre gli strumenti hardware e software necessari per la prevenzione, la rilevazione, l'analisi e la risposta agli incidenti;
- dotare il personale degli strumenti di lavoro necessari per operare anche all'esterno delle sedi aziendali;
- predisporre le procedure e la documentazione tecnica di supporto necessaria;
- eseguire valutazioni dei rischi periodiche;
- applicare le misure di prevenzione stabilite;

- assicurare che il personale sia adeguatamente formato e competente.

4.2 Rilevazione e analisi

Gli eventi potenzialmente riconducibili a incidenti di sicurezza possono essere rilevati tipicamente attraverso le seguenti modalità:

- rilevazione da parte del personale aziendale (dipendenti o collaboratori);
- notifica ricevuta dai sistemi di monitoraggio dell'organizzazione;
- segnalazione ricevuta da clienti/utenti, fornitori o altri soggetti esterni (es. CSIRT nazionale).

Il personale aziendale che dovesse rilevare un evento potenzialmente riconducibile a un incidente di sicurezza, è tenuto a segnalarlo immediatamente all'Area aziendale competente, così come definito al § 3. Nei casi di eventi che abbiano una significativa probabilità di procurare danni fisici ai lavoratori o di comprometterne la salute, tale segnalazione deve essere effettuata solo dopo aver abbandonato la propria postazione di lavoro e aver raggiunto condizioni di sicurezza secondo quanto previsto nelle procedure definite nei Piani di emergenza aziendali.

A seguito di una rilevazione proattiva o della ricezione di una segnalazione, un addetto dell'Area aziendale competente analizza l'evento al fine di valutare se si sia effettivamente in presenza di un incidente di sicurezza. Gli incidenti di sicurezza possono coinvolgere sia l'ambito informatico sia altri ambiti (es. documenti cartacei, comunicazioni orali). Alcuni esempi di incidenti possono essere i seguenti:

- malware su una postazione di lavoro;
- furto o smarrimento di una postazione di lavoro;
- sottrazione di dati da un database;
- defacing di un sito web;
- compromissione di un asset ICT e suo utilizzo per svolgere attività illecite;
- accesso non autorizzato a un asset ICT;
- intercettazione o manomissione di autenticazioni o sessioni web;
- interruzione o degrado delle prestazioni di un servizio ICT;
- guasto o malfunzionamento di un asset ICT;
- danneggiamento di un asset ICT;
- disastro naturale o ambientale;
- furto di documentazione cartacea;
- distruzione di documentazione cartacea;
- rivelazione a soggetti non autorizzati di informazioni riservate.

Nel caso in cui sia confermato l'incidente, si provvede alla sua classificazione in termini di gravità utilizzando la tabella di riferimento riportata di seguito:

GRAVITA'	IMPATTO
1 - Irrilevante	L'incidente provoca: - effetti non rilevanti sui servizi dell'organizzazione; - violazioni di informazioni "pubbliche" o di valore trascurabile.
2 - Significativo	L'incidente provoca: - degrado o interruzione di servizi "non essenziali"; - degrado di servizi "essenziali" - violazioni di informazioni aziendali "a uso interno".

3 - Grave	L'incidente provoca: - interruzione di servizi "essenziali" percepita da un numero limitato di utenti; - violazioni di informazioni aziendali "riservate", dati personali "comuni" o quantità limitate di dati personali "particolari".
4 - Disastroso	L'incidente provoca: - danni alle persone; - interruzione di servizi "essenziali" percepita da un numero significativo o dalla totalità degli utenti; - violazioni di informazioni aziendali "strettamente riservate" o quantità significative di dati personali "particolari".

TABELLA 2

Nota. I servizi "essenziali" vengono identificati attraverso un'analisi di impatto sul business e sono riportati all'interno del "Piano di continuità operativa aziendale".

Quindi l'incidente viene registrato nel sistema di trouble ticketing aziendale. Tale registrazione può essere effettuata in un momento successivo in caso di eventi di disastro che richiedano l'immediato abbandono della postazione di lavoro o di problemi tecnici ad accedere al sistema di trouble ticketing.
Il sistema di trouble ticketing costituisce una knowledge base relativa alla gestione degli incidenti e consente di poter reperire informazioni sulle azioni effettuate e i relativi autori in caso di contestazioni da parte dei clienti/utenti o in sede giudiziale. I ticket relativi agli incidenti devono essere conservati per un periodo adeguato per garantire la disponibilità delle informazioni in caso di indagini e procedure giudiziarie (di norma 36 mesi) e preservati da distruzione, perdita, modifica o accesso non autorizzato.
In caso di incidente classificato "grave" o "disastroso" il soggetto che ha effettuato l'analisi informa il proprio Responsabile/Viceresponsabile di Area e il proprio Direttore/Vicedirettore di Divisione o Coordinatore di Aggregato.
In caso di incidente classificato "disastroso", secondo quanto definito nel "Piano di continuità operativa aziendale (§ 5.2)", il Direttore/Vicedirettore di Divisione o Coordinatore di Aggregato competente valuta l'appropriatezza della classificazione assegnata all'incidente: quando confermata, attiva il Comitato di crisi; in caso contrario abbassa il livello di classificazione. Il Comitato di crisi dichiara lo stato di emergenza e assume il controllo di tutte le operazioni e la responsabilità sulle decisioni per affrontare l'emergenza, ridurne l'impatto e ripristinare le condizioni preesistenti.

4.3 Contenimento e acquisizione di evidenze digitali di reato

4.3.1 Contenimento

Il contenimento ha lo scopo di limitare la diffusione o il danno causato dall'incidente e può essere di due tipologie: a breve termine o a lungo termine. Il contenimento non è applicabile in tutte le tipologie di incidente.
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 dalla rete dei sistemi coinvolti.

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 per finalità di analisi interne o per un eventuale prosieguo in ambito legale 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.
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. Alcuni esempi di operazioni di contenimento a lungo termine sono:

- 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.

4.3.2 Acquisizione di evidenze digitali di reato

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 i sistemi informativi dell'organizzazione;
- interruzione di servizi pubblici essenziali;
- violazioni della privacy di utenti e cittadini;
- utilizzo illegale dei sistemi per perpetrare truffe o diffondere materiale illecito.

L'attività di acquisizione forense delle evidenze digitali di reato deve essere effettuata il prima possibile, onde evitare eventuali alterazioni apportate in fase di investigazione, e richiede di:

- identificare tutti i sistemi che possono essere stati compromessi o su cui sia possibile raccogliere eventuali evidenze digitali di reato;
- effettuare le copie delle evidenze digitali di reato in modo valido dal punto di vista forense, affinchè possano essere utilizzabili in un processo giuridico;
- conservare le copie delle evidenze digitali di reato per un periodo di 36 mesi o fino alla conclusione delle azioni legali avviate, preservandole da distruzione, perdita, modifica o accesso non autorizzato;
- mantenere una documentazione cronologica ("catena di custodia") di tutte le operazioni eseguite per l'acquisizione, la movimentazione e la conservazione delle copie delle evidenze digitali di reato, comprensiva di orari, autori e localizzazione dei supporti di memorizzazione, onde evitare in un eventuale ambito giudiziale possibili contestazioni sulla correttezza delle operazioni eseguite.

Per effettuare tali operazioni tipicamente è opportuno ricorrere a un fornitore specializzato.

4.4 Rimozione e ripristino

4.4.1 Rimozione

Dopo che un incidente è stato contenuto, può essere necessario eliminarne tutte le componenti e identificare e mitigare le vulnerabilità che sono state sfruttate. A tale scopo è fondamentale identificare tutti i sistemi coinvolti.
Le attività eseguite in questa fase possono essere per esempio:

- rimozione del malware;
- cancellazione dei file o dati malevoli o compromessi;
- disabilitazione delle utenze compromesse.

La rimozione non è applicabile in tutte le tipologie di incidente e, in alcuni casi, può essere effettuata durante il ripristino.

4.4.2 Ripristino

Il ripristino consiste nel riportare i sistemi alla normale operatività, confermarne il funzionamento e risolvere eventuali vulnerabilità per prevenire futuri incidenti simili. Il ripristino può richiedere azioni tipo:

- sostituzione del componente guasto;
- risoluzione del malfunzionamento;
- attivazione del sistema nel sito di disaster recovery;
- restore del sistema da un backup pulito;
- ricostruzione del sistema (es. reinstallazione del sistema operativo);
- ripristino dei file compromessi con versioni pulite;
- installazione di patch o aggiornamenti di sistema e/o applicativi;
- modifiche di password;
- restringimento del perimetro di sicurezza della rete (es. regole su firewall, acl su apparati di rete).

In caso di incidente “disastroso” il ripristino deve essere effettuato sulla base delle strategie e soluzioni e nel rispetto degli obiettivi descritti nel “Piano di continuità operativa aziendale”. Le attività operative necessarie per il ripristino vengono svolte dalle Aree aziendali competenti. Queste sono organizzate in modo da assicurare la presenza di personale reperibile anche nel caso in cui l’evento si presenti al di fuori del normale orario lavorativo e possono avvalersi di fornitori esterni con i quali siano stati precedentemente stipulati contratti con opportuni livelli di servizio. Eventuali acquisti di beni o servizi in condizioni di urgenza devono essere autorizzati dal Direttore Generale. Durante lo svolgimento delle attività di ripristino l’Area aziendale competente mantiene costantemente aggiornato il proprio Direttore/Vicedirettore di Divisione o Coordinatore di Aggregato, che a sua volta informa il Comitato di crisi.

4.5 Comunicazioni, notifiche, denunce

4.5.1 Comunicazioni interne ed esterne

In caso di incidente “grave” l’Area aziendale competente per il servizio o il relativo Direttore/Vicedirettore di Divisione o Coordinatore di Aggregato devono effettuare tempestivamente una segnalazione agli utenti interessati contenente una prima valutazione dell'incidente e la tempistica prevista per il ripristino della normale operatività. Una volta

risolto l'incidente, deve essere effettuata una nuova comunicazione per informare dell'avvenuto ripristino e fornire una descrizione dell'incidente, del relativo impatto e della durata.
In caso di incidente "disastroso" il Comitato di crisi valuta la necessità di effettuare opportune comunicazioni rivolte al personale aziendale, ai clienti, agli utenti, ai fornitori o ai media e ne definisce contenuti e modalità.

4.5.2 Notifiche di violazioni di dati personali

Nel caso in cui si riscontri una violazione di dati personali di cui Lepida ScpA è Titolare, il Direttore Generale o altro soggetto delegato dallo stesso deve richiedere un parere al RPD relativamente alla necessità di effettuare la notifica al Garante per la protezione dei dati personali ed eventualmente agli interessati. La decisione ultima al riguardo è di competenza del Direttore Generale e deve derivare da una valutazione dei rischi che la violazione dei dati personali presenta per i diritti e le libertà degli interessati coinvolti.
L'eventuale notifica al Garante deve essere effettuata senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui l'organizzazione ne è venuta a conoscenza, utilizzando il modello messo a disposizione dal Garante stesso, ed essere sottoscritta dal Direttore Generale. Essa deve contenere:

- natura della violazione;
- categorie e numero approssimativo di registrazioni di dati personali coinvolte;
- categorie e numero approssimativo di interessati coinvolti;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio o attenuare i possibili effetti negativi della violazione;
- nome e dati di contatto del RPD.

Oltre tale termine la notifica deve essere corredata delle ragioni del ritardo. Nei casi in cui si disponga di informazioni solo parziali relative alla violazione, deve essere effettuata una notifica preliminare, cui deve seguire una notifica integrativa non appena saranno a disposizione tutte le informazioni necessarie.
Quando ritenuto necessario dall'organizzazione o nel caso in cui venga richiesto dal Garante, deve essere effettuata anche una notifica agli interessati. Questa deve avvenire il prima possibile utilizzando le modalità di comunicazione ritenute più opportune (es. e-mail, pubblicazione di un avviso sul sito Internet aziendale).

Qualora la violazione riguardi trattamenti di dati per i quali Lepida ScpA è stata designata Responsabile o Sub-Responsabile, il Direttore/Vicedirettore di Divisione competente, il Coordinatore di Aggregato competente o il Direttore Generale devono effettuare una notifica rispettivamente al Titolare o al Responsabile, entro 24 ore dalla rilevazione, se non diversamente specificato nell'accordo tra le parti, contenente:

- natura della violazione;
- categorie e numero approssimativo di registrazioni di dati personali coinvolte;
- categorie e numero approssimativo di interessati coinvolti;
- recapiti del RPD nominato;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio o attenuare i possibili effetti negativi della violazione.

4.5.3 Notifiche di incidenti relativi al servizio di Identity Provider SPID

Nel caso in cui si riscontri un incidente di sicurezza relativo al servizio di Identity Provider SPID erogato da Lepida ScpA, è necessario classificare ulteriormente l'incidente utilizzando la seguente tabella di riferimento, come previsto nel "Regolamento recante le modalità attuative per la realizzazione dello SPID":

CLASSIFICAZIONE	DESCRIZIONE
1 - Comportamento anomalo e non circoscritto	Comportamento difforme dalle regole tecniche per il quale non è circoscritto il potenziale impatto (codice 1A, se rilevato dal gestore; codice 1B, se rilevato da terzi).
2 - Comportamento anomalo circoscritto	Comportamento difforme dalle regole tecniche per il quale è circoscritto il potenziale impatto (codice 2A, se rilevato dal gestore; codice 2B, se rilevato da terzi).
3 - Malfunzionamento bloccante	Tipologia di malfunzionamento a causa del quale le funzionalità del sistema del gestore delle identità digitali, come definite nelle regole tecniche, non possono essere utilizzate in tutto o in parte consistente dagli utenti (codice 3A, se rilevato dal gestore; codice 3B, se rilevato da terzi).
4 - Malfunzionamento grave	Tipologia di malfunzionamento a causa del quale in alcune circostanze le funzionalità del sistema del gestore delle identità digitali, come definite nelle regole tecniche, possono essere utilizzate parzialmente dagli utenti (codice 4A, se rilevato dal gestore; codice 4B, se rilevato da terzi).
5 - Malfunzionamento	Situazione a causa della quale le funzionalità del sistema del gestore delle identità digitali, come definite nelle regole tecniche, in tutto o in parte, risultano degradate ovvero il sistema ha un comportamento anomalo in situazioni circoscritte e per funzionalità secondarie (codice 5A, se rilevato dal gestore; codice 5B, se rilevato da terzi).

TABELLA 3

Per i disservizi contraddistinti dai codici 1A, 1B, 2A, 2B, 3A o 3B il Direttore/Vicedirettore della Divisione Software & Piattaforme Enti & Sanità deve effettuare una comunicazione all'Agenzia per l'Italia Digitale (AgID) entro trenta minuti dalla rilevazione; per quelli contraddistinti dai codici 4A, 4B, 5A o 5B entro due ore. La comunicazione deve contenere una prima valutazione dell'incidente, le eventuali azioni adottate o che si prevede di adottare e la tempistica prevista per il ripristino della normale operatività.
In caso di violazione di dati personali deve essere effettuata una notifica al Garante per la protezione dei dati personali, e per conoscenza ad AgID, entro 24 ore dalla rilevazione, in modo sufficientemente dettagliato. Quando ritenuto necessario dall'organizzazione o nel caso in cui venga richiesto dal Garante, deve essere effettuata anche una notifica agli interessati il prima possibile.

4.5.4 Denunce alle Forze dell'Ordine

Nel caso in cui si riscontri un incidente con possibili risvolti di natura penale il Direttore/Vicedirettore di Divisione o Coordinatore di Aggregato competente o altro soggetto delegato dal Direttore Generale sono tenuti, previa condivisione con il Direttore Generale, ad effettuare la denuncia alle Forze dell'Ordine.

4.6 Attività post-incidente

Per ogni incidente "grave" o "disastroso" o riconducibile a violazioni di dati personali, al servizio di Identity Provider SPID o a potenziali reati, oltre alla segnalazione agli organi di competenza da notificare entro le 24 ore dal momento della sua rilevazione, deve essere prodotto un rapporto di incidente dettagliato (utilizzando il modulo allegato al presente documento) entro le 24 ore successive il completamento delle attività di rimozione/ripristino. Il rapporto deve essere sottoscritto dal Direttore/Vicedirettore di Divisione o Coordinatore di Aggregato competente o dal Direttore Generale e trasmesso in formato pdf al Responsabile dell'Area Monitoraggio & Sicurezza. Quest'ultimo provvede a conservare detti rapporti per un periodo di 36 mesi e a preservarli da distruzione, perdita, modifica o accesso non autorizzato; inoltre mantiene aggiornato un registro contenente l'elenco degli incidenti registrati.

Al fine di migliorare il processo adottato per la gestione degli incidenti e le misure tecniche applicate, gli incidenti più significativi devono essere analizzati durante incontri periodici che prevedono la partecipazione del Direttore/Vicedirettore di Divisione o Coordinatore di Aggregato competente o del Direttore Generale, del Responsabile dell'Area Monitoraggio & Sicurezza e degli ulteriori soggetti interessati. Durante tali incontri è opportuno porsi le seguenti domande:

- esattamente cosa è successo e quando?
- l'incidente è stato gestito correttamente? Sono state seguite le procedure predisposte? Tali procedure sono risultate adeguate? Sono state coinvolte le persone giuste? Sono state effettuate azioni che hanno ritardato il ripristino?
- che cosa potrebbe essere fatto diversamente in un analogo incidente futuro?
- come potrebbe essere migliorato lo scambio di informazioni all'interno dell'organizzazione e con l'esterno?
- quali misure di sicurezza potrebbero prevenire incidenti simili in futuro?
- quali eventi o indicatori potrebbero essere osservati in futuro per rilevare incidenti simili?
- quali misure di sicurezza potrebbero migliorare la rilevazione e la risposta ad analoghi incidenti futuri?

I principali punti discussi, le decisioni prese e le eventuali approvazioni necessarie da parte del Direttore Generale devono essere documentati.

5. Responsabilità dei fornitori e di ulteriori soggetti esterni

Tutti i fornitori e gli ulteriori soggetti esterni che erogano nei confronti di Lepida ScpA servizi che possono comprendere attività di rilevazione, analisi e risposta agli incidenti di sicurezza, sono tenuti, nei limiti delle responsabilità e delle modalità operative definite a livello contrattuale, ad effettuare tali attività in conformità con quanto riportato nel presente documento e a mantenere costantemente aggiornata Lepida ScpA sul loro svolgimento, in

particolar modo ogni qualvolta siano necessarie azioni da parte della stessa.

I fornitori e gli ulteriori soggetti esterni che, in esecuzione del contratto, effettuano trattamenti di dati personali di cui Lepida ScpA è Titolare o Responsabile, sono designati rispettivamente Responsabili o Sub-Responsabili del trattamento ai sensi dell'art. 28 del Regolamento U.E. n. 679/2016. Gli oneri e le responsabilità conseguenti a tale designazione sono disciplinati in uno specifico accordo parte integrante del contratto. Nel caso in cui rilevi una violazione di dati personali, il fornitore o il soggetto esterno è tenuto a:

- effettuare le attività di analisi e risposta agli incidenti, nei limiti delle responsabilità e delle modalità operative definite a livello contrattuale, secondo quanto previsto nel presente documento;
- effettuare una notifica a Lepida ScpA entro 24 ore dalla rilevazione contenente:
    - natura della violazione;
    - categorie e numero approssimativo di registrazioni di dati personali coinvolte;
    - categorie e numero approssimativo di interessati coinvolti;
    - recapiti del RPD nominato o del soggetto competente della gestione della violazione;
    - descrizione delle probabili conseguenze della violazione dei dati personali;
    - descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio o attenuare i possibili effetti negativi della violazione.

Allegato - Rapporto incidente di sicurezza

RAPPORTO INCIDENTE DI SICUREZZA	
INFORMAZIONI DI SINTESI	
CODICE IDENTIFICATIVO INCIDENTE	
DESCRIZIONE DELL'INCIDENTE	
DATA/ORA DI INIZIO INCIDENTE	
DATA/ORA DI CHIUSURA INCIDENTE	
GRAVITA' ASSEGNATA (IRRILEVANTE, SIGNIFICATIVO, GRAVE, DISASTROSO)	
INFORMAZIONI DI DETTAGLIO	
DATA/ORA E MODALITA' ATTRAVERSO LE QUALI SI E' VENUTI A CONOSCENZA DELL'INCIDENTE	
CAUSA DELL'INCIDENTE	
SERVIZI, RISORSE IT O DATI COINVOLTI E RELATIVA UBICAZIONE	
CLIENTI/UTENTI COINVOLTI E CONSEGUENZE DELL'INCIDENTE SUGLI STESSI	
DURATA EFFETTIVA DEL DISSERVIZIO	
EVENTUALI ULTERIORI INFORMAZIONI RILEVANTI	
INFORMAZIONI AGGIUNTIVE IN CASO DI VIOLAZIONI DI DATI PERSONALI	
RUOLO DI LEPIDA (TITOLARE, RESPONSABILE O SUB-RESPONSABILE)	
CATEGORIE DI DATI PERSONALI COINVOLTI	
CATEGORIE DI INTERESSATI COINVOLTI	
NUMERO DI INTERESSATI / VOLUME DI DATI PERSONALI COINVOLTI	

CONSEGUENZE EFFETTIVE O PROBABILI DELLA VIOLAZIONE SUGLI INTERESSATI	
MISURE ADOTTATE A SEGUITO DELL'INCIDENTE	
MISURE TECNICHE E ORGANIZZATIVE ADOTTATE PER MITIGARE E PORRE RIMEDIO ALL'INCIDENTE	
MISURE TECNICHE E ORGANIZZATIVE ADOTTATE O DI CUI SI PROPONE L'ADOZIONE PER PREVENIRE SIMILI INCIDENTI FUTURI	
ALTRE INFORMAZIONI	
EVENTUALE ATTIVAZIONE COMITATO DI CRISI AZIENDALE	
EVENTUALE SEGNALAZIONE A SOGGETTI ESTERNI (FORZE DELL'ORDINE, GARANTE PRIVACY, INTERESSATI, TITOLARE O RESPONSABILE DEL TRATTAMENTO, AGID, ALTRI)	

_____ , lì _____

_____
(nome e cognome)