Procedura per la gestione degli incidenti di sicurezza delle informazioni

PRO-SGSI-001 ver. 7.4

Sommario

1. Scopo e campo di applicazione

Il presente documento descrive il processo adottato da Lepida per la gestione degli incidenti di sicurezza delle informazioni che possono coinvolgere gli asset utilizzati, i servizi erogati e/o i dati trattati dall'organizzazione.

Il processo di gestione degli incidenti di sicurezza delle informazioni ha lo scopo di:

- assicurare che gli incidenti siano rilevati e gestiti con la massima tempestività al fine di minimizzarne l'impatto;
- assicurare che gli incidenti siano comunicati agli utenti coinvolti e ai soggetti istituzionali preposti secondo quanto previsto dalle normative e dai regolamenti vigenti;
- migliorare continuamente la maturità dell'organizzazione nella gestione degli incidenti.

Sono tenuti a conoscere e ad applicare quanto riportato nel presente documento tutti i dipendenti di Lepida, nonché i propri collaboratori e fornitori.

2. Definizioni

Nel presente documento si applicano le seguenti definizioni:

- Evento di sicurezza: qualsiasi situazione che potrebbe causare conseguenze negative sugli asset o i servizi dell'organizzazione o sulla disponibilità, integrità o riservatezza dei dati trattati;
- Incidente di sicurezza: evento o insieme di eventi di sicurezza che in modo conclamato causano conseguenze negative sugli asset o i servizi dell'organizzazione o sulla disponibilità, integrità o riservatezza dei dati trattati. Gli incidenti di sicurezza possono comportare violazioni di dati personali;
- Violazione di dati personali (o data breach): 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 (cfr. Regolamento UE 2016.679 - GDPR).

3. Ruoli e Responsabilità

3.1 Soggetti preposti alla gestione operativa degli incidenti

Il "soggetto preposto all'analisi degli eventi/incidenti di sicurezza" ha le seguenti responsabilità:

- presidiare in modo continuativo i sistemi informatici di monitoraggio e gli alert generati dagli stessi;
- effettuare attività di verifica periodiche (es. analisi dei log dei sistemi), al fine di identificare anomalie;
- ricevere segnalazioni di eventi di sicurezza dal personale interno o da soggetti esterni (es. clienti, utenti, fornitori, CSIRT);
- analizzare gli eventi di sicurezza rilevati e identificare gli incidenti di sicurezza;
- determinare la tipologia, la severità e la priorità di trattamento degli incidenti di sicurezza;
- registrare gli incidenti di sicurezza attraverso opportuni strumenti;
- attivare il "soggetto preposto al trattamento degli incidenti di sicurezza" competente per ambito;
- informare il proprio Direttore in caso di incidenti di severità grave o critica.

Il "soggetto preposto al trattamento degli incidenti di sicurezza" è responsabile di:

- individuare ed attuare idonee azioni di contenimento, investigazione, rimozione e ripristino;
- coinvolgere ulteriori soggetti interni o esterni competenti per specifiche attività di contenimento, investigazione, rimozione o ripristino;
- verificare, dopo il ripristino, l'effettivo ritorno alla normale operatività, possibilmente con il coinvolgimento dell'utilizzatore finale;
- informare e mantenere aggiornati i soggetti interni responsabili degli specifici asset o servizi coinvolti e l'help desk competente per ambito;
- mantenere aggiornato il proprio Direttore in caso di incidenti di severità grave o critica;
- predisporre, a incidente risolto, un incident report, comprensivo delle lezioni apprese e delle azioni di miglioramento individuate.

All'interno dell'organizzazione aziendale di Lepida, ciascuna Area può essere preposta all'analisi o al trattamento degli incidenti di sicurezza in base alle loro specificità. Tuttavia le Aree tipicamente coinvolte e i relativi ambiti di competenza sono riportati nella seguente tabella.

AREA	**DIPARTIMENTO / DIVISIONE**	**AMBITO DI COMPETENZA**
01 - Affari Interni & Segreteria	DG - Direzione Generale	Locali aziendali a Bologna e Parma
14 - Attivazione & Esercizio Reti 15 - Manutenzione Reti	D1 - Dipartimento Reti	Siti, infrastrutture, apparati e servizi di rete

23 - Servizi IT 24 - Attivazione & Esercizio DC & Cloud 25 - Realizzazione & Manutenzione DC & Cloud	D2 - Dipartimento Datacenter & Cloud	Locali, infrastrutture, sistemi e servizi di data center; strumenti e servizi informatici aziendali
34 - Interoperabilità & Manutenzione Piattaforme & Servizi 35 - Attivazione & Esercizio Piattaforme & Servizi	D3 - Dipartimento Software & Piattaforme Enti & Sanità	Piattaforme e servizi applicativi
45 - Digitalizzazione & Dematerializzazione	D4 - Dipartimento Integrazioni Digitali	Locali e archivi cartacei a Minerbio e Granarolo; servizi di integrazione digitale
54 - Attivazione & Esercizio Welfare	D5 - Dipartimento Welfare Digitale	Servizi di welfare digitale
94 - Supporto ai Contatti e all'Accesso	D9 - Dipartimento Accesso	Servizi di accesso alle prestazioni sanitarie
A1 - Monitoraggio & Sicurezza	DA - Divisione Sicurezza, Ambiente & Emergenza	Sistemi e servizi di cybersecurity

TABELLA 1

3.2 Direttori

Tutti i Direttori di Lepida hanno le seguenti responsabilità:

- definire idonee strategie per la gestione degli incidenti di sicurezza di competenza;
- informare e mantenere aggiornati gli altri Direttori, il Direttore Generale e il Responsabile della Protezione dei Dati Personali in caso di incidenti di severità grave o critica;
- assicurare idonee comunicazioni verso i soggetti esterni coinvolti in caso di incidenti di severità grave o critica;
- effettuare le notifiche verso i soggetti istituzionali preposti secondo quanto previsto dalle normative e dai regolamenti vigenti;
- approvare e formalizzare mediante sottoscrizione gli incident report di propria competenza ed impegnarsi a mettere in atto, compatibilmente con la disponibilità delle risorse economiche necessarie, le azioni di miglioramento previste negli stessi;
- assicurare che il personale aziendale, i collaboratori e i fornitori sotto la propria responsabilità conoscano ed attuino diligentemente la presente procedura.

3.3 Direttore Generale

Al Direttore Generale di Lepida competono le seguenti responsabilità:

- autorizzare qualsiasi azione e spesa straordinaria necessaria per la gestione degli incidenti di sicurezza;
- approvare qualsiasi comunicazione e notifica relativa agli incidenti di sicurezza effettuata da Lepida verso l'esterno;
- delegare soggetti interni a rappresentare Lepida o ad effettuare comunicazioni e notifiche formali verso soggetti istituzionali.

3.4 Responsabile della Protezione dei Dati Personali

Il Responsabile della Protezione dei Dati Personali (RPD) designato da Lepida ha la responsabilità di fornire, ove richiesto, il proprio parere in relazione all'adeguatezza delle misure di sicurezza applicate per la protezione dei dati personali e alla necessità di effettuare la notifica al Garante per la Protezione dei Dati Personali (GPDP), ed eventualmente agli interessati, in caso di data breach.

3.5 Personale aziendale

Tutto il personale di Lepida è tenuto a:

- segnalare tempestivamente qualsiasi potenziale incidente di sicurezza causato o di cui venga a conoscenza al proprio Responsabile e all'indirizzo email uls@lepida.it;
- fornire massima collaborazione al personale preposto alla gestione degli incidenti di sicurezza.

3.6 Collaboratori e fornitori

Tutti i collaboratori e i fornitori di Lepida sono tenuti a:

- segnalare tempestivamente qualsiasi potenziale incidente di sicurezza causato o di cui vengano a conoscenza al proprio Referente in Lepida o all'indirizzo email uls@lepida.it;
- attuare le azioni di gestione degli incidenti di sicurezza indicate nella presente procedura, sulla base di quanto previsto dai requisiti contrattuali e dalle modalità operative concordate con Lepida;

- fornire massima collaborazione al personale preposto da Lepida alla gestione degli incidenti di sicurezza.

4. Rilevazione e analisi degli incidenti di sicurezza

4.1 Rilevazione

Il processo di gestione degli incidenti di sicurezza si attiva quando uno dei "soggetti preposti all'analisi degli eventi/incidenti di sicurezza" rileva un evento (o un insieme di eventi) di sicurezza.

Tipicamente la rilevazione può avvenire a seguito di:

- alert prodotti dai sistemi informatici di monitoraggio;
- anomalie riscontrate durante attività di verifica (es. analisi dei log dei sistemi, audit);
- segnalazioni ricevute dal personale interno o da soggetti esterni (es. clienti, utenti, fornitori, CSIRT).

4.2 Analisi

A seguito della rilevazione dell'evento (o insieme di eventi) di sicurezza, il "soggetto preposto all'analisi degli eventi/incidenti di sicurezza" ne effettua l'analisi, avvalendosi degli strumenti e delle procedure operative in uso all'interno dell'Area di appartenenza.

La prima parte dell'analisi ha lo scopo di comprendere se l'evento possa essere categorizzabile come incidente di sicurezza, escludendo eventuali falsi positivi, o se, pur non essendo categorizzabile come tale, richieda ugualmente un trattamento per mitigare il rischio che da esso possa derivare un incidente (tale trattamento non è descritto nel presente documento). Gli incidenti e gli eventi che richiedono un trattamento vengono registrati sul sistema di trouble ticketing.

Nel caso in cui l'evento sia categorizzato come incidente di sicurezza, l'analisi prosegue per determinarne la tipologia, la severità e la priorità di trattamento.

La tipologia viene assegnata utilizzando la seguente tabella di riferimento.

TABELLA DI CLASSIFICAZIONE DEGLI INCIDENTI PER TIPOLOGIA	
Tipologia	**Descrizione**
Operativo accidentale	Incidenti causati da azioni o eventi accidentali.

	Esempi: errori di processo, errori umani, errori software, guasti hardware, danneggiamenti accidentali di infrastrutture o dispositivi, smarrimenti di dispositivi, eventi naturali o ambientali.
Operativo intenzionale	Incidenti causati da azioni intenzionali non riconducibili ad attacchi informatici. Esempi: accessi non autorizzati a locali o a dati, furti di dispositivi o dati, diffusioni non autorizzate di dati, manomissioni o danneggiamenti intenzionali di infrastrutture o dispositivi, violazioni intenzionali di norme o regolamenti.
Cyber	Incidenti causati da attacchi informatici. Esempi: malware o ransomware, attacchi di denial of service, intrusioni o compromissioni di reti, sistemi, applicazioni o dati, defacing di siti web, attacchi di social engineering o phishing, furti di identità digitali, intercettazione o dirottamento di sessioni o comunicazioni, esfiltrazioni di dati, attacchi alla supply chain.

TABELLA 2

La severità viene stabilita tramite una valutazione dei possibili impatti che l'incidente sta causando o potrebbe causare sull'erogazione dei servizi e sulla disponibilità, integrità o riservatezza dei dati, e delle possibili conseguenze che potrebbe provocare a livello societario-istituzionale, economico e reputazionale. L'incidente viene classificato in termini di severità sulla base del più grave degli impatti e delle conseguenze che potrebbe causare secondo quanto previsto nella seguente tabella di riferimento.

TABELLA DI CLASSIFICAZIONE DEGLI INCIDENTI PER SEVERITA'				
	Severità			
Impatto / Conseguenza	**Incidente critico**	**Incidente grave**	**Incidente significativo**	**Incidente minore**
Impatto sui servizi	Indisponibilità di uno o più servizi di "livello 1" (vedi Tabella seguente) percepita dalla totalità o da un numero significativo di utenti di durata	Indisponibilità di uno o più servizi di "livello 1" (vedi Tabella seguente) percepita dalla totalità o da un numero significativo di	Indisponibilità di uno o più servizi NON di "livello 1" percepita dalla totalità o un numero significativo di utenti	Indisponibilità di uno o più servizi NON di "livello 1" percepita da un numero limitato di utenti indipendentemente dalla durata

	superiore a 1 ora	utenti di durata uguale o inferiore a 1 ora, oppure percepita da un numero limitato di utenti indipendentemente dalla durata	indipendentemente dalla durata	
Impatto sui dati	Distruzione, perdita, modifica o accesso non autorizzati, divulgazione o furto di grandi quantità di dati personali o dati classificati "riservati" dall'organizzazione	Distruzione, perdita, modifica o accesso non autorizzati, divulgazione o furto di limitate quantità di dati personali o dati classificati "riservati" dall'organizzazione	Distruzione, perdita, modifica o accesso non autorizzati, divulgazione o furto di grandi quantità di dati classificati "a uso interno" dall'organizzazione e non contenenti dati personali	Distruzione, perdita, modifica o accesso non autorizzati, divulgazione o furto di limitate quantità di dati classificati "a uso interno" dall'organizzazione e non contenenti dati personali
Conseguenze a livello societario-istituzionale	Atti formali di rilievo nei confronti della Società da parte degli Enti Soci o di esponenti istituzionali, a seguito dell'incidente			
Conseguenze a livello economico	Costi, di qualsiasi natura, causati dall'incidente superiori a €500.000	Costi, di qualsiasi natura, causati dall'incidente tra €50.000 e €500.000		
Conseguenze a livello reputazionale	Articoli fortemente negativi su media con visibilità a livello nazionale o regionale, a seguito dell'incidente	Articoli fortemente negativi su media con visibilità a livello locale, a seguito dell'incidente		

TABELLA 3

I servizi di "livello 1" sono quelli valutati più critici per il business tramite Business Impact Analysis (BIA) e vengono elencati nella seguente tabella.

SERVIZI "DI LIVELLO 1"	
	Servizio
Servizi di rete	Collegamento a Internet della rete Lepida Connettività dei data center regionali su rete Lepida Connettività di sedi primarie di AUSL e Aziende Ospedaliere su rete Lepida DNS pubblico della rete Lepida Housing di operatori TLC nei siti POP della rete Lepida e nei data center regionali Rete radiomobile regionale ERretre Trasporto di operatori TLC su rete Lepida
Servizi di data center	BAAS/CBAAS Database Oracle Firewall Housing di Enti nei data center regionali Server virtuali Storage
Piattaforme applicative	Accesso unitario Anagrafe Regionale Assistiti (ARA) Anagrafe Vaccinale Regionale (AVR) Cartella Clinica Assistenziale (CCA) Cartella SOLE Centro Unico Prenotazione (CUP) Docer Fascicolo Sanitario Elettronico (FSE) Federa Icarer Infrastruttura SOLE LepidaID Payer Sistema Accoglienza Regionale (SAR) Sistema Informativo Sanità Penitenziaria (SISP)
Servizi a uso interno	Active Directory Google Workspace Firewall

TABELLA 4

La priorità di trattamento degli incidenti viene assegnata sulla base della severità identificata: maggiore è la severità, maggiore deve essere la priorità.

Una volta determinate la tipologia, la severità e la priorità dell'incidente, il "soggetto preposto all'analisi degli eventi/incidenti di sicurezza" coinvolge il "soggetto preposto al trattamento degli incidenti di sicurezza" competente per ambito.

In caso di incidente classificato con livello di severità "grave" o "critico", il "soggetto preposto all'analisi degli eventi/incidenti di sicurezza" informa i soggetti interni responsabili degli specifici asset o servizi interessati e il proprio Direttore. Quest'ultimo provvede a metterne al corrente gli altri Direttori e il RPD attraverso il gruppo WhatsApp denominato "Direttori Lepida ScpA".

5. Trattamento degli incidenti di sicurezza

Il "soggetto preposto al trattamento degli incidenti di sicurezza" competente per ambito, identifica ed implementa le azioni di trattamento dell'incidente ritenute ottimali, avvalendosi degli strumenti e delle procedure operative in uso all'interno dell'Area di appartenenza. Il trattamento può richiedere il coinvolgimento di ulteriori soggetti interni o esterni. Nel caso in cui le azioni da porre in atto presentino un carattere di invasività o possano comportare un disservizio più grave di quello in essere, deve essere richiesta l'autorizzazione al Direttore competente.

In caso di incidenti disastrosi che compromettano la continuità dell'operatività dell'organizzazione occorre attenersi a quanto previsto nei Piani di Continuità Operativa e di Disaster Recovery aziendali.

Nel corso del trattamento, in considerazione delle ulteriori informazioni acquisite e dell'evoluzione dell'intervento, la classificazione dell'incidente in termini di tipologia, severità e priorità assegnata in fase di analisi iniziale può essere modificata.

Il trattamento dell'incidente può essere scomposto nelle seguenti quattro fasi, sebbene non sempre siano possibili o necessarie tutte e quattro:

- contenimento;
- investigazione;
- rimozione;
- ripristino.

5.1 Contenimento

Il contenimento è finalizzato a limitare la diffusione dell'incidente, a mitigarne i danni sugli asset interessati e ad attuare soluzioni temporanee che consentano il ripristino, seppure parziale, del servizio. Pertanto, quando possibile e necessario, deve essere attuato il prima possibile.

A titolo esemplificativo le azioni di contenimento in caso di incidente cyber possono includere:

- disconnessione dalla rete dei sistemi coinvolti;
- creazione di regole sul firewall atte a bloccare l'accesso ai sistemi coinvolti;
- disabilitazione di un account utente o dei suoi privilegi;
- modifiche sul sistema DNS;
- arresto di servizi o processi malevoli.

E' opportuno attuare solo azioni di contenimento che non alterino i sistemi coinvolti, nei casi in cui siano necessarie successive azioni di investigazione o acquisizione di evidenze digitali.

5.2 Investigazione

L'investigazione consiste nell'identificazione della causa dell'incidente e delle alterazioni apportate agli asset durante l'evoluzione dell'incidente fino a quel momento.

In caso di incidenti cyber essa prende il nome di digital forensics e prevede le seguenti fasi:

- identificazione dei sistemi da analizzare;
- acquisizione dei dati dai dispositivi o sistemi interessati: può essere live, ovvero a sistema acceso, o post mortem, ovvero a sistema spento;
- analisi delle tracce digitali;
- produzione del report contenente i risultati dell'analisi.

La digital forensics è particolarmente importante in presenza di reati informatici, al fine di poter disporre di prove da utilizzare in sede giudiziaria. In tal caso, affinché le prove possano essere considerate valide in giudizio, è necessario che siano acquisite e conservate tramite tecniche che consentano di trattare in maniera idonea il dato informatico, preservandolo da alterazioni, e di garantire il mantenimento continuo della catena di custodia.

5.3 Rimozione

La rimozione consiste nell'eliminazione della causa dell'incidente e delle alterazioni apportate agli asset individuate in fase di investigazione.

Alcuni esempi di azioni di rimozione in caso di incidenti cyber sono i seguenti:

- rimozione di malware;
- cancellazione di file malevoli o compromessi;
- disabilitazione di account utente;
- ripristino della baseline di configurazione di sistema;
- installazione di patch per eliminare vulnerabilità.

5.4 Ripristino

Il ripristino consiste nel riportare alla normale operatività gli asset e i servizi coinvolti dall'incidente.

Per gli incidenti cyber il ripristino può avvenire, ad esempio, attraverso le seguenti azioni:

- restore di un sistema o un database da un backup;
- reinstallazione dell'immagine di un sistema;
- attivazione del servizio nel sito di disaster recovery.

Il ripristino si considera completato dopo verifica dell'effettivo ritorno alla normale operatività, effettuata possibilmente con il coinvolgimento dell'utilizzatore finale.

6. Comunicazioni e notifiche

6.1 Comunicazioni interne

In presenza di incidenti "gravi" o "critici" il "soggetto preposto al trattamento degli incidenti di sicurezza" tiene aggiornati sull'evoluzione dell'incidente, fino alla risoluzione, il proprio Direttore, i soggetti interni responsabili degli specifici asset o servizi interessati e l'help desk competente per ambito, affinchè quest'ultimo possa fornire risposta a eventuali segnalazioni o lamentele da parte degli utenti.

6.2 Comunicazioni esterne

In caso di incidenti "gravi" o "critici" vengono effettuate opportune comunicazioni, subito dopo la rilevazione, durante il trattamento e a conclusione del ripristino, volte ad informare e mantenere aggiornati Enti, operatori, cittadini e media, secondo le modalità definite nel "Piano di comunicazione di incidenti critici".

6.3 Notifiche di violazioni di dati personali

Eventuali violazioni di dati personali vengono trattate secondo quanto previsto dal Regolamento UE 2016.679 - GDPR (Artt. 33 e 34).

Nel caso in cui si riscontri una violazione di dati personali di cui Lepida è Titolare, viene valutato il rischio per i diritti e le libertà delle persone fisiche interessate causato dalla violazione e acquisito un parere dal RPD.

A meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche interessate, viene effettuata una notifica al GPDP senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui l'organizzazione ne è venuta a conoscenza, attraverso il portale dedicato del GPDP https:..servizi.gpdp.it.databreach.s.. Oltre tale termine la notifica viene corredata dei motivi del ritardo. Nei casi in cui si disponga di informazioni solo parziali relative alla violazione, viene effettuata una notifica preliminare, seguita da una notifica integrativa quando risultano disponibili tutte le informazioni necessarie. Quando la violazione dei dati personali viene valutata dal Titolare suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche interessate, vengono informati anche gli interessati senza ingiustificato ritardo, utilizzando il canale di comunicazione ritenuto più opportuno a seconda delle circostanze.

Qualora la violazione riguardi trattamenti di dati per i quali Lepida è stata designata Responsabile, viene effettuata una notifica al Titolare, senza ingiustificato ritardo, entro i termini specificati nell'accordo di designazione o entro 24 ore dalla rilevazione, qualora non definiti.

6.4 Notifiche di incidenti relativi al servizio di Identity Provider SPID

Lepida, in qualità di Identity Provider SPID erogatore del servizio LepidaID, è tenuta ad inviare ad AgID notifiche di incidenti, malfunzionamenti o interruzioni di servizio secondo quanto previsto all'Art. 30 del "Regolamento recante le modalità attuative per la realizzazione dello SPID" (v.2, 22.07.2016) e nelle "Indicazioni per la notifica di incidenti, malfunzionamenti e interruzioni di servizio" (SV_QM_Notfiche_1.0, 21.12.2021).

Nel caso in cui si rilevi un incidente (che nella definizione utilizzata nel presente contesto include anche i malfunzionamenti e le interruzioni di servizio) relativo al servizio LepidaID o agli asset utilizzati per la sua erogazione, viene ulteriormente classificato in termini di severità, in aggiunta

alla classificazione effettuata secondo le modalità descritte al § 4.2, e notificato ad Agid secondo le definizioni e le tempistiche riportate nella tabella seguente.

SEVERITÀ'	DESCRIZIONE	TEMPI DI NOTIFICA AD AGID
Impatto alto	E' interessata la gran parte o la totalità degli utenti del provider	Entro 30 minuti dalla rilevazione
Impatto medio	E' interessata una parte degli utenti del provider	Entro 30 minuti dalla rilevazione
Impatto lieve	Sono interessati asset del provider ma senza impatto sulle funzionalità principali	Entro 2 ore dalla rilevazione

TABELLA 5

Le notifiche sono effettuate attraverso il portale dedicato di AgID https:..trustservices.agid.gov.it. Nei casi in cui si disponga di informazioni solo parziali relative all'incidente, viene effettuata una notifica preliminare, seguita da una notifica integrativa quando risultano disponibili tutte le informazioni necessarie.

In presenza di violazioni di dati personali, viene anche effettuata una notifica al GPDP entro 24 ore dalla rilevazione per una prima sommaria comunicazione ed entro 72 ore dalla rilevazione per una comunicazione dettagliata. Le notifiche sono effettuate attraverso il portale dedicato del GPDP https:..servizi.gpdp.it.databreach.s.. Inoltre, qualora dalla violazione possa derivare un pregiudizio ai dati personali o alla riservatezza di un utente o di altre persone cui si riferiscono i dati violati, viene effettuata una comunicazione a tali soggetti senza ingiustificato ritardo.

7. Attività post-incidente

A seguito della risoluzione dell'incidente è prevista la predisposizione di un Incident Report. Tale attività è obbligatoria per gli incidenti "gravi" o "critici", raccomandata per gli incidenti "significativi".

Per l'Incident Report deve essere utilizzato il template allegato al presente documento, che richiede di inserire anche le lezioni apprese (lessons learned) e le conseguenti azioni migliorative, già attuate a seguito dell'incidente o che il Direttore competente si impegna a mettere in atto, compatibilmente con la disponibilità delle risorse economiche necessarie.

Il "soggetto preposto al trattamento degli incidenti di sicurezza" predispone l'Incident Report e lo sottopone alla verifica del proprio Direttore e del Direttore della Divisione DA. Al più entro 7 giorni dal completamento del ripristino, il Direttore competente firma digitalmente il Report e lo trasmette al Direttore della Divisione DA e al Direttore Generale. Sulla base delle informazioni riportate nel Report, la Divisione DA censisce l'incidente nel "Registro incidenti di sicurezza" aziendale e, in caso di violazione di dati personali, anche nel "Registro dei data breach" aziendale. I Report vengono conservati dalla Divisione DA per un periodo non inferiore a 36 mesi.

Nel caso in cui un cliente coinvolto in un incidente "grave" o "critico" richieda a Lepida un Incident Report, il Direttore competente, con il supporto del Direttore della Divisione DA, predispone un Incident Report a uso esterno, a partire da quello ad uso interno. Successivamente il Direttore competente sottopone il Report alla validazione del Direttore Generale e lo trasmette al cliente, al più entro 7 giorni dalla richiesta.

Periodicamente il Direttore Generale chiede conto ai Direttori dello stato di attuazione delle azioni migliorative previste negli Incident Report.

Allegato - Template di incident report

lepida	**TEMPLATE INCIDENT REPORT**	MOD-SGSI-001 Ver. 7.4 del 13.06.2023

INCIDENT REPORT

Codice identificativo	*Inserire il codice identificativo dell'incidente, utilizzando la seguente codifica: INC-aaaammgg-numprog, dove:* • *aaaammgg: anno mese e giorno di rilevazione dell'incidente* • *numprog: numero progressivo per distinguere più incidenti rilevati il medesimo giorno (di default 1)*
Data e ora inizio	*Inserire data (gg/mm/aaa) e ora (hh:mm) in cui l'incidente ha avuto inizio*

Data e ora rilevazione	*Inserire data (gg/mm/aaa) e ora (hh:mm) in cui l'incidente è stato rilevato*
Data e ora fine	*Inserire data (gg/mm/aaa) e ora (hh:mm) in cui l'incidente è stato risolto*
Tipologia	*Inserire la tipologia dell'incidente, scegliendo tra: operativo accidentale, operativo intenzionale o cyber, sulla base della tabella di riferimento riportata nella Procedura per la gestione degli incidenti di sicurezza*
Severità	*Inserire la severità dell'incidente, scegliendo tra: minore, significativo, grave o critico, sulla base della tabella di riferimento riportata nella Procedura per la gestione degli incidenti di sicurezza*
Descrizione	*Descrivere sinteticamente l'incidente, includendo gli asset/servizi/dati coinvolti, gli utenti/clienti interessati e l'impatto/durata* *Nel caso in cui siano coinvolti asset/servizi/dati sotto la responsabilità di differenti Dipartimenti/Divisioni aziendali, ciascuno di essi deve descrivere gli asset/servizi/dati, gli utenti/clienti interessati e l'impatto/durata di propria competenza*
Asset/servizi coinvolti	*Inserire schematicamente gli asset/servizi coinvolti dall'incidente* *Nel caso in cui siano coinvolti asset/servizi sotto la responsabilità di differenti Dipartimenti/Divisioni aziendali, ciascuno di essi deve inserire gli asset/servizi di propria competenza*
Dati coinvolti	*Inserire schematicamente i dati coinvolti dall'incidente, laddove applicabile* *Nel caso in cui siano coinvolti dati sotto la responsabilità di differenti Dipartimenti/Divisioni aziendali, ciascuno di essi deve inserire i dati di propria competenza*
Utenti/clienti interessati	*Inserire schematicamente gli utenti/clienti o le aree geografiche interessate dall'incidente* *Nel caso in cui siano coinvolti asset/servizi/dati sotto la responsabilità di differenti Dipartimenti/Divisioni aziendali, ciascuno di essi deve inserire gli utenti/clienti di propria competenza*
Rilevazione	*Descrivere sinteticamente la modalità con cui è stato rilevato l'incidente, la relativa data e ora e, se presente, un*

	ticket ID di riferimento sul sistema di trouble ticketing aziendale
Causa	*Descrivere sinteticamente la causa dell'incidente individuata*
Trattamento	*Descrivere sinteticamente le principali azioni di trattamento dell'incidente (mitigazione, investigazione, rimozione, ripristino) attuate, comprensive di data e ora*
Comunicazioni/notifiche formali	*Descrivere le eventuali comunicazioni/notifiche formali effettuate a seguito dell'incidente verso utenti/clienti o soggetti istituzionali (es. GPDP, AgID), comprensive di data e ora*
Lezioni apprese e azioni migliorative	*Descrivere sinteticamente le lezioni apprese (lessons learned) dall'incidente e le azioni migliorative già attuate a seguito dell'incidente o che il Direttore competente si impegna a mettere in atto, compatibilmente con la disponibilità delle risorse economiche necessarie*
Eventuali note aggiuntive	*Inserire eventuali note aggiuntive*

Data

Inserire data di emissione

Direttore competente

Inserire nome e cognome
(firmato digitalmente)

Storia del documento				
Ver.	**Autore**	**Verifica**	**Approvazione**	**Commenti**
7.3	Area Gestione del Rischio & Qualità (24.04.2022)	Tutti i Direttori (28.04.2022)	Direttore Generale (02.05.2022)	Aggiornamento
7.4	Direttore Divisione Sicurezza, Ambiente e Emergenza (13.06.2023)	Tutti i Direttori (26.06.2023)	Direttore Generale (13.07.2023)	Revisione generale e aggiornamento modalità di notifica ad AgID in caso di incidenti relativi al servizio LepidaID