FLOWE S.p.A. SB
Policy Incident Management

Consiglio di Amministrazione del 26/07/2023

1 INDICE

1 PREMESSA

1.1 CONTESTO DI RIFERIMENTO

Scopo del presente documento è fornire una guida per i dipendenti di Flowe (di seguito anche la Società), Capogruppo e fornitori esterni, per garantire una risposta adeguata ed una pronta segnalazione degli incidenti operativi e di sicurezza.

I principi richiamati nella presente *policy* trovano attuazione nella Procedura operativa, nella quale saranno espressi in dettaglio i compiti, le attività e i controlli finalizzati a garantire il processo di gestione degli incidenti operativi e di sicurezza.

1.2 AMBITO DI RIFERIMENTO

Come dettagliato nelle relative procedure operative, la gestione degli incidenti operativi e di sicurezza si raccorda con il processo di continuità operativa e di *disaster recovery* predisposto per gli incidenti relativi alla disponibilità dei servizi, compresi i gravi incidenti di sicurezza informatica.

Il processo di gestione degli incidenti comprende le fasi di Rilevamento, Valutazione e registrazione, Monitoraggio e risoluzione e Attività Post-Incidente, al fine di raggiungere i seguenti obiettivi:

- assicurare che siano utilizzati metodi e procedure ben definiti per garantire una risposta rapida ed efficiente al manifestarsi di un incidente
- aumentare la trasparenza e la comunicazione relativamente agli incidenti nei confronti degli attori coinvolti nel processo
- assicurare il soddisfacimento dei requisiti di conformità relativi alla gestione degli incidenti[1], con particolare riferimento a:
- attivare le procedure di escalation in caso di crisi.

La presente *Policy* descrive gli adempimenti indispensabili che la Società deve adottare per la gestione efficace degli incidenti, anche qualora riguardino soggetti terzi coinvolti nel ciclo operativo della Società.

Con riferimento alla "*Policy sulle modalità di redazione, approvazione, diffusione ed aggiornamento della normativa interna*" del Gruppo, il documento si colloca al primo livello (di vertice) della piramide documentale richiamata nello schema seguente.

[1] "provvedimento Banca d'Italia 22 febbraio 2022 (Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica)";
"Istruzioni Per La Segnalazione Dei Gravi Incidenti Operativi O Di Sicurezza – IP E IMEL" di Banca d'Italia;
"Orientamenti in materia di segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (PSD2)";
"Regolamento Europeo in materia di protezione dei dati personali 2016/679" (General Data Protection Regulation – GDPR);
"Disposizioni di vigilanza per le banche – Circolare n.285 del 2013 e successivi aggiornamenti.

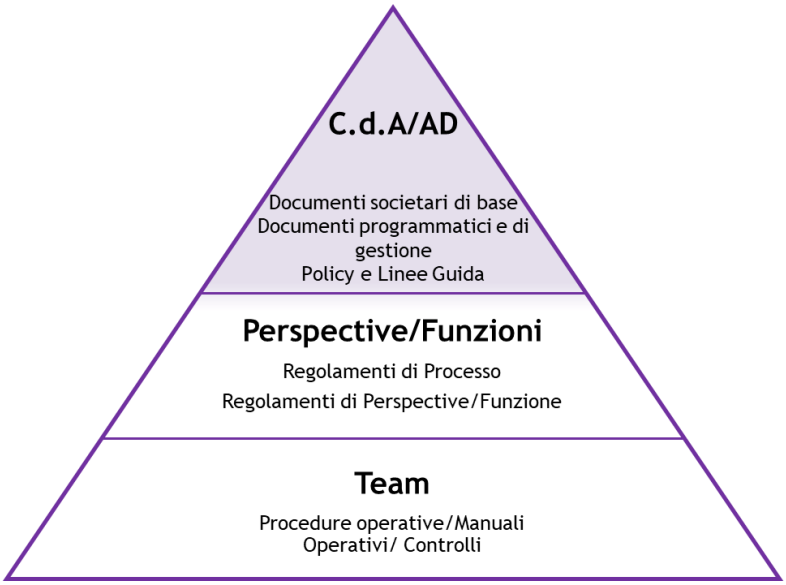

Figura 1: Modello della normativa interna di riferimento

2 APPLICABILITÀ

2.1 DESTINATARI DEL DOCUMENTO

Il Presente documento si applica a tutte le Perspective di Flowe.

2.2 RESPONSABILITÀ DEL DOCUMENTO

L'aggiornamento e la revisione del presente documento sono di responsabilità del team IT Operation Security & Governance con cadenza almeno annuale. Ogni modifica o integrazione sostanziale del documento deve essere approvata dal Consiglio di Amministrazione della Società.

3 DEFINIZIONI

Minaccia: potenziale causa di un incidente indesiderato, che può comportare danni a un sistema o a un'organizzazione.

Evento informatico: qualsiasi evento osservabile in un sistema o in una rete. Un evento potrebbe indicare un malfunzionamento di una componente informatica standard e, quindi, fungere da innesco per la generazione di un incidente.

Incidente operativo o di sicurezza: ogni evento, o serie di eventi collegati, non pianificati dalla banca che ha, o probabilmente avrà, un impatto negativo sull'integrità, la disponibilità, la riservatezza, e/o l'autenticità dei servizi. Nel dettaglio:

- **incidenti operativi** derivanti da processi inadeguati o malfunzionanti, persone e sistemi o

eventi di forza maggiore. Tra tali eventi sono inclusi quelli naturali, errori software/hardware, eventi accidentali, malfunzionamenti di processo, sabotaggio (attacco fisico);

- **incidenti di sicurezza**, compresi i cyber**,** derivanti da attività volontaria e malevola di threat actors esterni o interni riguardanti l'accesso, l'uso, la divulgazione, l'interruzione, la modifica o la distruzione non autorizzata delle risorse della Società o incidenti che comunque producono, anche involontariamente, diffusione e/o alterazione di dati riservati della clientela e/o dell'intermediario:
  - accesso o utilizzo non autorizzato di dati o risorse;
  - utilizzo inappropriato delle risorse;
  - interruzione o compromissione intenzionale di servizi di calcolo o telecomunicazione;
  - alterazione o corruzione non autorizzata di risorse o dati memorizzati o in transito.

Grave incidente operativo o di sicurezza (Major): un incidente operativo o di sicurezza da cui derivi o è probabile che derivi almeno una delle seguenti conseguenze:

a. perdite economiche elevate o prolungati disservizi per l'intermediario, anche a seguito di ripetuti incidenti di minore entità;

b. disservizi rilevanti sulla clientela e altri soggetti (ad es., intermediari o infrastrutture di pagamento); la valutazione della gravità considera il numero dei clienti o controparti potenzialmente coinvolti e l'ammontare a rischio;

c. il rischio di inficiare la capacità della banca di conformarsi alle condizioni e agli obblighi di legge o previsti dalla disciplina di vigilanza;

d. danni reputazionali, nel caso venga reso di pubblico dominio (ad esempio attraverso i media e gli organi di stampa).

Minor incident: un incidente operativo o di sicurezza con un basso impatto sulla Società. Tale incidente riguarda un singolo utente o reparto e potrebbe avere già una risoluzione documentata. Tali incidenti dovrebbero essere gestiti in maniera efficiente al fine di evitare che consumino eccessive risorse.

Incidente Handler: personale abilitato della Perspective incaricato della raccolta, registrazione, gestione e reporting dell'incidente operativo o di sicurezza.

Glossario

- PIS - *Payment Initiation Service:* servizio di disposizione di ordini di pagamento;
- AIS - *Account Information Service*: servizio di informazione sui conti;
- API - *Application Program Interface:* interfaccia di programmazione delle applicazioni;
- ASPSP - *Account Servicing Payment Service Provider*: prestatore di servizi di pagamento di radicamento del conto;
- *Integrità*: proprietà della salvaguardia dell'esattezza e completezza delle risorse (inclusi i dati);
- *Disponibilità*: proprietà dei servizi connessi ai pagamenti di essere accessibili e utilizzabili da parte degli utenti dei servizi di pagamento;
- *Riservatezza*: proprietà per cui le informazioni non sono rese disponibili o divulgate a persone, entità o procedure non autorizzate;
- *Autenticità*: proprietà di una fonte di essere quella che dichiara di essere;
- *Data Breach* - una violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- *DPO - Data Protection Officer* ha la funzione di affiancare titolare, addetti e responsabili del trattamento affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni

della normativa vigente in materia di protezione dei dati personali.

- *Continuità*: proprietà delle procedure, attività e risorse di un'organizzazione funzionali all'erogazione dei servizi connessi ai pagamenti di essere pienamente fruibili e operative a livelli di servizio accettabili e predefiniti.

4 ATTORI, RUOLI E RESPONSABILITÀ

Il modello organizzativo adottato dalla Società per la gestione degli incidenti viene declinato internamente, in linea con le principali pratiche di settore.

Si prevede che l'evento possa essere segnalato da tutti i dipendenti, i fornitori esterni ed i clienti della Società. Il personale abilitato delle Perspective, in qualità di Incidet Handler, garantisce la registrazione e la classificazione puntuale dell'incidente, anche al fine di individuare l'attore coinvolto per la successiva fase di risposta all'incidente.

Nel caso l'incidente abbia impatto rilevante su risorse informatiche utilizzate sia dalla Banca che da Flowe, attraverso l'unità organizzativa identificata al proprio interno come responsabile della gestione del grave incidente , si prevede l'ingaggio dell'unità organizzativa della Capogruppo referente delle attività di segnalazione ed il Responsabile Operativo della Crisi di Banca Mediolanum (che svolgono in outsourcing servizi aziendali in virtù di un apposito accordo di esternalizzazione), al fine di concordare sulla classificazione dell'incidente ed eventualmente predisporre i report per l'Autorità di Vigilanza.

4.1 INCIDENT HANDLER

Il personale abilitato delle Perspective *Banking Services & Controls* ed Augmented Intelligence incaricato di ricevere segnalazioni sugli eventi sia internamente che esternamente, esaminare i dati dell'eventuale incidente, classificare l'incidente e registrarlo su strumenti di monitoraggio dedicato, ingaggiare eventualmente il fornitore esterno o il team interno per la risposta all'incidente, raccogliere informazioni sullo stato di avanzamento dell'incidente, analizzare i dati relativi all'incidente per identificarne la causa e le lesson learned, viene qualificato quale Incident Handler.

4.2 CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione di Flowe ha la responsabilità di approvare la presente *Policy* e deliberare i successivi aggiornamenti.

Il CdA è informato tempestivamente in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti del sistema informativo; ed è aggiornato su impatto, misure correttive e controlli aggiuntivi a seguito di tali eventi.

4.3 AMMINISTRATORE DELEGATO

L'Amministratore Delegato ha la responsabilità di:

- definire la struttura organizzativa a supporto del processo di gestione degli incidenti, assicurandone nel tempo la rispondenza alla strategia aziendale;
- garantire il corretto dimensionamento quali-quantitativo del personale impiegato nelle attività di gestione degli incidenti;
- approvare il disegno del processo di gestione degli incidenti;
- presidiare l'attività di gestione della continuità operativa a fronte di un incidente;

- assumere decisioni tempestive in merito a gravi incidenti operativi o di sicurezza di cui è prontamente informato, e fornire informazioni al CdA in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti, con particolare riferimento all'impatto, alla risposta e ai controlli supplementari da definire.

4.4 PERSPECTIVE AUGMENTED INTELLIGENCE

'*Augmented Intelligence',* in qualità di incident handler, ha la responsabilità di:

- presidiare i supporti tecnologici predisposti per la registrazione e gestione del processo di gestione degli incidenti;
- ricevere tutte le segnalazioni relative agli incidenti operativi e di sicurezza "rilevanti" inerenti ai servizi di pagamento elettronico e avviare, con il supporto delle unità organizzative coinvolte e delle strutture di controllo, la raccolta dei dati necessari alla relativa valutazione di impatto;
- predisporre la proposta di classificazione/riclassificazione dell'incidente grave, da sottoporre al Comitato di Gestione della Crisi di Flowe, sulla base dei parametri e delle soglie previste dalle istruzioni per la segnalazione dei gravi incidenti ai sensi delle disposizioni di Vigilanza per le banche classificate come "Significant";
- gestire gli incidenti operativi o di sicurezza, per i quali, in ragione della loro particolare natura, non sia necessario coinvolgere il fornitore per la risposta operativa all'incidente;
- effettuare un controllo di secondo livello sulla classificazione degli incidenti effettuata dalle altre *Perspective* in fase di registrazione;
- in qualità di referente della Capogruppo per i gravi incidenti *di sicurezza*, ingaggia il Settore IT Security della Capogruppo e le trasmette i dati e le informazioni necessarie nei tempi e nei modi definiti e condivisi per la predisposizione dei *report* alle Autorità competenti;
- informare tempestivamente l'Unità di Supporto Manageriale IT User Support & Service Management, *owner* del processo di *Incident Management* della Capogruppo, di tutti i gravi incidenti operativi o di sicurezza rilevati;
- fornire, al Comitato di Crisi di Flowe tutti gli elementi utili per deliberare in merito alla proposta di classificazione dell'incidente (es. totale delle transazioni interessate, numero dei pagamenti compromessi);
- presidiare il processo di risoluzione dell'incidente qualora esso sia stato individuato all'interno del perimetro della Società;
- garantire, fino alla completa risoluzione dell'incidente, un costante follow-up delle azioni intraprese e delle tempistiche di risoluzione nei confronti dei clienti, delle Funzioni aziendali coinvolte, degli outsourcer e dell'Amministratore Delegato della Società;
- segnalare all'Ufficio Privacy di Banca Mediolanum le eventuali violazioni degli obblighi di tutela delle informazioni personali e riservate delle quali Flowe è titolare del trattamento;
- registrare e archiviare tutti i dati, con il supporto di *Perspective* terze, utilizzati a presidio e valutazione della tipologia e della classe di Incidente, degli impatti nonché i documenti e report prodotti per le eventuali segnalazioni a Banca d'Italia;
- attivare il Responsabile Operativo della Gestione della Crisi della Capogruppo al fine di coordinare le valutazioni sui possibili impatti dell'incidente sulla Capogruppo (es.: legali/reputazionali) e valutare la necessità di convocare il Comitato di Gestione della Crisi ovvero prevedere un'informativa;
- segnalare all'Ufficio Privacy di Banca Mediolanum i *data breach* rilevati nel corso della propria attività o segnalati da altre *Perspective;*
- contribuire a ridurre attraverso attività di analisi dell'incidente, congiuntamente agli altri incident handler coinvolti, la probabilità di accadimento e l'impatto degli incidenti attraverso le attività di root cause analysis e leasson learned;
- registrare adeguatamente tutte le informazioni necessarie relative all'*incident*;
- effettuare la *due diligence* sui fornitori di sistemi e servizi ICT prima della stipula del contratto, verificando le procedure di gestione degli incidenti operativi e di sicurezza, tra cui la notifica e l'attivazione dei livelli successivi di intervento.

4.5 PERSPECTIVE *BANKING SERVICES & CONTROLS*

La Perspective, in qualità di incident handler, ha la responsabilità di:

- definire e aggiornare con il supporto degli altri attori coinvolti la presente Policy, le relative procedure operative e metriche di controllo e i processi correlati, verificandone la corretta applicazione anche da parte degli outsourcer e garantendo il presidio delle attività degli stessi per quanto riguarda l'erogazione dei servizi forniti;
- segnalare eventuali incidenti operativi o di sicurezza desumibili a partire da segnalazioni ricevute dalla clientela;
- classificare, secondo i criteri definiti dalla normativa interna, gli incidenti che impattano o potrebbero impattare la Società;
- registrare l'aggiornamento dello stato di avanzamento di gestione dell'incidente;
- fornire supporto informativo alla Perspective '*Augmented Intelligence*' nel corso dell'intero processo di gestione dell'incidente in particolare per quanto riguarda:
    - il coinvolgimento degli *outsourcer* coinvolti nella risposta all'incidente, con l'obiettivo rafforzare il monitoraggio attivo del ciclo di vita dell'incidente;
    - il f*ollow-up* nei confronti dei clienti, delle Funzioni aziendali coinvolte, degli outsourcer e del *Comitato di Crisi*;
- definire le eventuali modalità di comunicazione nei confronti dei clienti;
- contribuire a ridurre attraverso attività di analisi dell'incidente, congiuntamente agli altri incident handler coinvolti, la probabilità di accadimento e l'impatto degli incidenti attraverso le attività di root cause analysis e lesson learned;
- archiviare le informazioni necessarie relative all'incidente sul tool di monitoraggio interno.

4.6 DIREZIONE INNOVAZIONE & PIANIFICAZIONE E SVILUPPO FLOWE DI BANCA MEDIOLANUM

La Direzione ha la responsabilità di supportare il processo di valutazione dell'incidente, al fine di individuare eventuali *major incident*, fornendo informazioni relative all'impatto economico.

4.7 BUSINESS ACCELERATION

Qualora sia necessario effettuare comunicazioni alla clientela, la perspective *Business Acceleration* collabora con la perspective *Banking Services & Controls* nella predisposizione dei contenuti delle comunicazioni e, in coordinamento con le altre unità previste dalla presente *policy*.

4.8 FUNZIONE RISK MANAGEMENT

La Funzione *Risk Management* verifica, raccoglie e riconcilia, con il supporto delle altre unità organizzative[2], le perdite rivenienti da rischi operativi oggetto di segnalazione periodica alle competenti Autorità di Vigilanza, coerentemente a quanto previsto dal *framework* di Basilea III.

Ha la responsabilità di supportare il processo di valutazione dell'incidente, al fine di individuare eventuali *major incident*. In particolare, dopo essere stata tempestivamente allertata, la Funzione fornisce supporto a *Augmented Intelligence* nella valutazione della gravità dell'incidente (in base all'impatto economico) e nella raccolta, presso le unità organizzative coinvolte, dei dati relativi ai costi associati all'incidente specifico, ai fini dell'integrazione dei dati necessari alla predisposizione

[2] Con riferimento agli incidenti rilevati dalla Società, l'Unità raccoglie le informazioni accedendo direttamente al supporto tecnologico utilizzato per il tracciamento degli incidenti e, ove necessario, richiede eventuali informazioni aggiuntive ai singoli attori coinvolti nel processo operativo di gestione degli incidenti.

delle segnalazioni all'Autorità di Vigilanza. Sono inclusi, i gravi incidenti operativi non legati ai servizi di pagamento, da segnalare alla Capogruppo.

Coordinandosi con le *Perspective Banking Services & Controls e la Direzione Innovazione & Pianificazione e Sviluppo Flowe di Banca Mediolanum* effettua una valutazione circa l'impatto reputazionale derivante dall'incidente rilevato.

4.9 FUNZIONE COMPLIANCE

La Funzione *Compliance* ha la responsabilità di fornire, ove richiesto, supporto consulenziale a '*Augmented Intelligence* nella valutazione in ordine ad eventuali violazioni di obblighi regolamentari derivanti dalle conseguenze dell'incidente.

4.10 COMITATO DI CRISI

Il *Comitato di Crisi di Flowe*, composto dall'*Amministratore Delegato*, dai responsabili di *Perspective*, dai responsabili delle strutture di controllo, dal Responsabile ICT e dal responsabile della *Business Continuity*:

- Esamina le evidenze dell'istruttoria condotta dalla Perspective Augmented Intelligence e delibera rispetto alla proposta di classificazione dell'incidente e alla relativa comunicazione da inoltrare all'Autorità di Vigilanza e alla clientela ove necessario.
- Approva eventuali riclassificazioni dell'incidente proposte dalla *Perspective Augmented Intelligence*;
- Nelle fasi successive alla prima segnalazione, viene informato in merito allo stato di risoluzione dell'incidente e alle analisi effettuate sui dati reali raccolti ai fini dell'invio dei rapporti di aggiornamento all'*Autorità di Vigilanza*.

4.11 UNITÀ ORGANIZZATIVE DELLA CAPOGRUPPO

Ingaggiato da *Augmented Intelligence* laddove questa rilevi un possibile *data breach*, l'*Ufficio Privacy* di Banca Mediolanum ha la responsabilità di:

- valutare l'impatto dell'incidente in termini di rischi per gli interessati coinvolti (sulla base di quanto previsto dalle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679);
- predisporre i contenuti della eventuale comunicazione di notifica da inviare all'Autorità Competente (Garante per la protezione dei dati personali);
- costituire uno specifico *data breach team* che informato dell'esito delle valutazioni sui rischi per i diritti e le libertà degli interessati (potenziali ed effettivi) determinati dal *data breach* è responsabile dell'identificazione delle azioni per contenere e/o minimizzare i rischi per gli interessati e prevenirne la replica.

L'*Unità Business Continuity Office & Digital Process Automation* di Banca Mediolanum:

- in caso di incidente il cui impatto possa attivare potenzialmente uno degli scenari di continuità operativa, preventivamente condivisi, valuta, sulla base delle regole definite e di concerto con l'IT Governance di Banca Mediolanum, la gravità dell'impatto dell'incidente; a tal proposito informa il Comitato di Crisi di Flowe per la definizione del relativo livello di emergenza/escalation e delle misure e/o delle azioni da adottare;
- supporta il responsabile Business Continuity e la *Perspective Augmented Intelligence* di Flowe nella predisposizione della documentazione utile al Comitato di Gestione della Crisi di Flowe;

- collabora alla compilazione delle segnalazioni all'*Autorità di Vigilanza* con particolare riguardo alle tempistiche e modalità dell'eventuale attivazione del piano di continuità operativa e/o del piano di Disaster Recovery;
- intraprende le opportune misure atte a garantire la continuità operativa della Società nel caso in cui un incidente generi un'indisponibilità del servizio.

L'*Unità di Supporto Manageriale Service Policy & Procedures*, all'interno della Direzione Service, Operations & ICT di Banca Mediolanum (per incidenti in tema PSD2) e *l'Unità IT Security* di Banca Mediolanum (per incidenti in tema di sicurezza):

- riceve tutte le segnalazioni relative agli incidenti operativi e di sicurezza "rilevanti" giunti dal Comitato di Crisi di Flowe;
- condivide con le altre unità organizzative coinvolte i contenuti dei "rapporti di segnalazione" da inviare all'Autorità di Vigilanza;
- monitora lo stato di risoluzione dell'incidente e di ripristino dell'operatività e completa la raccolta dei dati ai fini della predisposizione ed inoltro all'Autorità di Vigilanza dei rapporti di segnalazione successivi (intermedio e finale);
- attiva gli opportuni canali per l'invio dei rapporti all'Autorità di Vigilanza.

4.12 PROVIDER DI SERVIZI ESTERNALIZZATI DALLA SOCIETÀ

I fornitori IT devono essere coinvolti nel processo di gestione degli incidenti coerentemente con la loro rilevanza nella gestione del servizio informativo. Devono, pertanto, essere definiti accordi contrattuali che comprendano livelli di servizio a supporto di una corretta gestione degli incidenti. Coerentemente con questa politica e con la normativa vigente, il coinvolgimento dei fornitori IT deve coprire i seguenti aspetti:

- supporto da parte dei fornitori IT anche in caso di incidenti rilevati della Società stessa;
- segnalazione alla Società interessata di incidenti rilevati dal fornitore IT aventi un impatto, anche potenziale, su sistemi e servizi a supporto dei processi della stessa, e relativa gestione, con particolare riferimento agli incidenti gravi per la società;
- produzione da parte del fornitore IT di reportistica a supporto degli incidenti della Società interessata, per la parte di propria competenza.

Devono quindi essere definite le procedure di comunicazione e coordinamento in caso di incidenti, in particolare nel caso di incidenti di sicurezza informatica.

In ogni caso, la Società deve anche essere informata su incidenti di sicurezza che interessino i servizi e le applicazioni in outsourcing.

Infine, i fornitori IT, nominati responsabili, che trattano dati personali di cui la Società è titolare sono tenuti a segnalare eventuali incidenti afferenti alla violazione dei dati personali (*data breach*) secondo le modalità operative definite dalla Società.

5 PRINCIPI DI INCIDENT MANAGEMENT

5.1 PRINCIPI GENERALI

Nell'ambito del processo di gestione sono individuati anche i soggetti e le funzioni coinvolte nella gestione degli incidenti o informati su di essi, con particolare riferimento ai gravi incidenti di sicurezza e ai casi di violazione di dati personali.

Ai fini del perseguimento degli obiettivi definiti, il processo di gestione degli incidenti deve:

1. facilitare la pronta rilevazione dell'incidente e la sua documentazione;
2. garantire che gli incidenti vengano gestiti da personale abilitato ed in possesso di adeguate competenze;
3. garantire che le evidenze degli incidenti siano documentate e manutenute all'interno di strumenti di raccolta, al fine di fornire informazioni per eventuali verifiche interne ed esterne;
4. assicurare la tempestiva comunicazione a tutte le Funzioni aziendali interessate dagli effetti dell'incidente e alle Funzioni per le quali è richiesta collaborazione;
5. rispettare la regolamentazione del settore, con particolare riferimento a quella di Banca d'Italia e la normativa interna della Società;
6. formalizzare ogni attività delegata e i livelli di servizio contrattualizzati con i fornitori, le modalità di comunicazione con la Società e le attività di controllo che il personale interno deve effettuare;
7. rispettare la gerarchia di escalation per garantire una tempestiva notifica degli incidenti e una corretta comunicazione al management delle Società impattate;
8. prevedere un controllo sistematico delle registrazioni degli incidenti per garantire una corretta categorizzazione e documentazione degli stessi, mettendola a disposizione anche delle Funzioni di controllo;
9. garantire attività di analisi sulle evidenze degli incidenti documentate, al fine di individuare root-cause analysis e lesson learned, utli per minimizzare la probabilità e l'impatto di accadimento di incidenti futuri;
10. adeguarsi con gli obiettivi previsti dall'Incident Response Plan, in termini di personale dedicato ed attività da espletare in caso di incidenti operativi e di sicurezza;
11. assicurare un'adeguata formazione del personale coinvolto nella gestione degli incidenti.

5.2 IDENTIFICAZIONE E CLASSIFICAZIONE DEGLI INCIDENTI

A valle di un'analisi specifica sull'evento informatico, dovrebbe essere definita una classificazione degli incidenti che possono impattare il sistema informativo della Società. La classificazione dovrebbe tener conto almeno degli impatti che tale incidente ha sulla disponibilità, sulla riservatezza e sull'integrità dei dati aziendali e del sistema informativo. La metodologia di classificazione degli incidenti è definita all'interno della P*rocedura Operativa di Incident Management*.

Devono essere in particolare identificati tempestivamente gli **incidenti gravi** al fine di attivare le appropriate procedure di *escalation,* che in caso di incidenti relativi alla disponibilità prevedono un raccordo con le procedure definite al riguardo nell'ambito della gestione della continuità operativa. Devono inoltre essere identificati i gravi incidenti di sicurezza informatica, che prevedono una specifica gestione nella procedura di *escalation*. La tempestiva rilevazione dell'incidente e la sua classificazione assume particolare rilevanza considerate le stringenti tempistiche di segnalazione dell'incidente all'Autorità Competente.

Inoltre, devono essere identificati tempestivamente gli **incidenti che comportano la violazione di dati personali**, conservati o comunque trattati dalla Società. Per tale tipologia di incidente è prevista una specifica gestione. In questo caso la tempestiva rilevazione dell'incidente e la sua classificazione in ambito "violazione di dati personali" (GDPR), assume particolare rilevanza considerata la tempistica entro la quale la segnalazione della violazione, nei casi di gravi conseguenze per gli interessati, deve essere fatta all'Autorità Competente (Garante per la protezione dei dati personali). Sono escluse da tale processo le possibili violazioni di dati personali rilevati presso i fornitori che sono Titolari del trattamento di dati personali dei soggetti. Tali eventi sono valutati e eventualmente, segnalati al Garante dallo stesso Titolare.

Infine, dovrebbe essere istituito e attuato un processo di segnalazione e gestione degli **incidenti Minor** in ambito ICT oltre che dei problemi per consentire una tempestiva gestione e risoluzione dell'evento che ha causato l'interruzione del processo e/o servizo da parte del personale abilitato. Tali incidenti, dovrebbero essere registrati e monitorati attraverso adeguati strumenti e presidi.

5.3 PROCEDURE DI ESCALATION E RACCORDO CON LE PROCEDURE DI CONTINUITÀ OPERATIVE

Le procedure di *escalation* in caso di incidenti gravi devono prevedere il raccordo con le procedure di gestione della crisi definite all'interno dei piani di continuità operativa della Società. La gestione degli incidenti comprende una procedura di *escalation*, come dettagliato nelle procedure operative che regolano la classificazione e la gestione degli incidenti, che descrivono le modalità del coinvolgimento dei ruoli e delle competenze necessarie per la corretta e tempestiva gestione dell'incidente e della convocazione del Comitato di Crisi per il governo dell'incidente. Nel dettaglio, i presidi di primo livello condividono l'anomalia di concerto con il responsabile della *Perspective Augmented Intelligence* di Flowe, che aggiorna il Comitato di Crisi di Flowe che include anche il *BCO* di Flowe per l'eventuale attivazione del *Piano di continuità operativa* ed informa la *Perspective Banking Services & Controls* per l'eventuale comunicazione agli utenti di business impattati. In caso di incidenti di sicurezza informatica classificati come eventi di violazione di dati personali si dovrà provvedere alla segnalazione dello stesso all'*Ufficio Privacy* di Banca Mediolanum che, unitamente al *DPO,* attiva le successive fasi di gestione del *data breach* secondo quanto previsto dai regolamenti interni.

La procedura di escalation non si attiva nel caso di incidenti minor e quindi classificati a basso impatto sulla Società. In tal caso, l'attività prosegue con il processo di gestione e monitoraggio degli incidenti ordinari in uso presso le Perspective competenti.

5.4 COMUNICAZIONE ALL'AUTORITÀ COMPETENTE ED AGLI ALTRI SOGGETTI INTERESSATI

I gravi incidenti operativi o di sicurezza sono comunicati tempestivamente all'Autorità Competente, secondo le modalità e i tempi previsti dalla normativa vigente e come descritto in dettaglio in apposita procedura[3].

Contestualmente, coerentemente con le politiche aziendali e con la normativa vigente, viene informato il Responsabile Operativo della Gestione della Crisi della Capogruppo. Gli incidenti successivamente riconosciuti dal *DPO* come violazioni di dati personali sono comunicati all'Autorità Competente (*Garante per la protezione dei dati personali*) secondo quanto previsto dal Regolamento del processo di gestione e segnalazione delle violazioni dei dati personali.

5.5 RACCORDO CON LE ATTIVITÀ DI MONITORAGGIO ED ALERTING DEL SISTEMA INFORMATIVO

La procedura di gestione degli incidenti si raccorda con i processi di monitoraggio del sistema informativo al fine di gestire tempestivamente gli incidenti rilevati.

Le attività di monitoraggio ed *alerting* del sistema informativo devono garantire un'adeguata alimentazione del processo di gestione degli incidenti. In particolare, le attività di monitoraggio di componenti critiche del sistema informativo devono garantire la rilevazione e la segnalazione tempestiva delle anomalie, nonché un'analisi delle stesse al fine di individuare gli incidenti in corso.

[3] Procedura Operativa di classificazione e segnalazione degli incidenti

Gli operatori di tutte le *Perspective* devono disporre di istruzioni operative atte a riconoscere e indirizzare correttamente le segnalazioni di incidenti e, in particolare, di incidenti *di sicurezza* da parte del personale interno.

5.6 ATTIVITÀ CORRETTIVE, ROOT-CAUSE ANALYSIS E LESSON LEARNED

Il processo di gestione deve assicurare che, in fase di chiusura dell'incidente, siano svolte le attività di analisi per l'individuazione delle azioni correttive necessarie a prevenire la replica dell'incidente o di incidenti simili e che sia avviata l'attuazione di tali azioni preventive.
Dovrebbe essere implementato un processo che preveda l'identificazione e l'eliminazione delle cause di fondo all'origine di un incidente informatico al fine di ridurre al minimo l'impatto degli eventi negativi, consentire un ripristino tempestivo ed evitare il verificarsi di incidenti ripetuti. Pertanto, dovrebbero essere analizzati sia gli incidenti operativi o di sicurezza individuati come impattanti per la società, sia quelli che si sono verificati all'interno e/o all'esterno dell'organizzazione.

La strategia di eliminazione delle root cause dovrebbe tenere in considerazione:

- gli interventi effettuati durante le attività di contenimento;
- la tipologia di incidente;
- il livello di gravità dell'incidente:
- la necessità di preservare le evidenze di quanto accaduto;
- il tempo massimo di indisponibilità prestabilito per gli asset informativi;
- gli strumenti di contrasto disponibili;
- una scala di priorità di intervento in base alla criticità degli asset informativi coinvolti.

Dovrebbero anche essere considerati gli insegnamenti fondamentali (lesson learned) appresi da queste analisi ed incorporati le modifiche derivanti da essi nelle attività di gestione degli incidenti, nelle procedure di risposta agli incidenti, nell'incidenti response plan e nella formazione del personale.

5.7 TRACCIATURA DEGLI INCIDENTI

Gli estremi degli incidenti sono registrati e documentati su specifici *tool* dall'Incident Handler, al fine di:

- definire la classificazione dell'incidente;
- facilitare la gestione dell'incidente e monitorarne lo stato avanzamento;
- consentire l'analisi a posteriori dell'incidente e raccogliere le lessons learned
- consentire alla Perspective Augmented Intelligence di avere a disposizione i dati necessari per avviare le eventuali attività di escalation e reporting, in caso di incidenti gravi

6 IL PROCESSO OPERATIVO DI GESTIONE DEGLI INCIDENTI

Il processo operativo di gestione e segnalazione degli incidenti operativi o di sicurezza si basa sul NIST Cybersecurity Framework e si articola nelle seguenti fasi:

- *rilevazione dell'evento (Identify);*
- *valutazione e registrazione dell'evento (Detect);*
- *monitoraggio e risoluzione dell'incidente (Respond);*
- *attività successive alla risoluzione dell'incidente (Recover).*

Per la descrizione di dettaglio delle singole attività si rimanda alle procedure operative che regolano la classificazione e la gestione degli incidenti.

Il processo è strutturato secondo livelli crescenti di competenze, in modo da prevedere il coinvolgimento di ruoli con potere decisionale adeguato alla gravità degli incidenti trattati.

7 NORMATIVA DI RIFERIMENTO

7.1 NORMATIVA INTERNA

- *Policy sulle modalità di redazione, approvazione, diffusione ed aggiornamento della normativa interna;*
- *Procedura Operativa Incident management;*
- *Procedura Operativa di classificazione e segnalazione degli incidenti.*

7.2 NORMATIVA ESTERNA

- D.lgs. 15 dicembre 2017, n. 218, "Recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta" e successivi aggiornamenti;
- Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica, provvedimento della Banca d'Italia del 23 luglio 2019 e successivi aggiornamenti;
- Orientamenti in materia di segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (PSD2), EBA GL 2021/03 e successivi aggiornamenti;
- Istruzioni per la segnalazione dei gravi incidenti operativi o di sicurezza–, Banca d'Italia;
- Disposizioni di vigilanza per le banche - Circolare Banca d'Italia n. 285 del 17 dicembre 2013 e successivi aggiornamenti;
- EBA/GL/2019/04. Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza;