FLOWE S.p.A. SB

Procedura Operativa Incident Management

INDICE

ENTRATA IN VIGORE POLICY		**DATA ULTIMO AGGIORNAMENTO**		**NUMERO VERSIONE**	
RESPONSABILE DEL DOCUMENTO	IT Operation, Security & Governance	**APPROVAZIONE DEL DOCUMENTO**		**APPLICABILITÀ DEL DOCUMENTO**	Dipendenti di Flowe, Capogruppo e fornitori esterni

STORICO VERSIONI

VERSIONE	APPROVATA DA	DATA DI REVISIONE	DESCRIZIONE DELLE MODIFICHE	AUTORE
1				
2			Classificazione degli incidenti (incidenti Minor), root cause analysis e lesson learned, processo dettagliato di gestione degli incidenti,	

1 OBIETTIVO DEL DOCUMENTO

Obiettivo del documento è illustrare la procedura di gestione degli incidenti che possono pregiudicare il normale funzionamento di tutti i processi operativi ed amministrativi di Flowe S.p.A. Società Benefit (di seguito anche Flowe o la Società). La presente Procedura esprime in dettaglio i compiti, le attività e i controlli finalizzati a garantire il processo di gestione degli incidenti operativi e di sicurezza, come definiti dalle disposizioni di vigilanza per gli IP e IMEL.

Per quanto riguarda gli *incident* di entità rilevante, la Società, conformemente alle disposizioni normative vigenti per gli Istituti di Moneta Elettronica e in attuazione della Direttiva 2015/2366/UE (PSD2) che richiede ai Prestatori di Servizi di Pagamento (PSP) di i) istituire procedure efficaci di gestione degli *incident*i e ii) di individuare e classificare gli incidenti gravi operativi o di sicurezza, ha definito uno specifico processo strutturato per la gestione dei *major incident*[1] in cui tempistiche, modalità di raccolta e trasmissione dei dati aggregati all'Autorità di Vigilanza sono conformi agli orientamenti emessi dall'EBA al riguardo e documentata nell'apposita Procedura Operativa Di Classificazione E Segnalazione Degli Incidenti.

Scopo del presente documento è di illustrare il processo di gestione degli incidenti, sia Major che Minor, in generale e più in dettaglio:

- descrivere ad alto livello le attività operative - in particolare, le modalità di rilevazione dell'evento, registrazione, gestione e chiusura dell'incidente - incluse le attività di controllo;
- indicare gli strumenti a supporto dell'operatività;
- descrivere le responsabilità delle unità organizzative di Flowe (in seguito anche *Perspective*) e degli altri attori coinvolti.

[1] Incidenti gravi secondo la definizione riportata da Banca d'Italia nelle Istruzioni per la Comunicazione degli Incidenti Operativi e di Sicurezza di IP e IMEL in vigore. Per la gestione di tali incidenti si rimanda alla "Procedura operativa di classificazione e segnalazione degli incidenti" di Flowe.

2 CONTESTO

La presente Procedura descrive le responsabilità e le azioni che gli attori individuati devono compiere al fine che la Società gestisca in maniera efficace ed efficiente gli incidenti operativi e di sicurezza. In particolare, vengono considerati diversi scenari:

- gestione degli incidenti *Minor*;
- gestione degli incidenti *Major*;

La presente Procedura è inserita all'interno del sistema delle fonti della normativa interna, come di seguito rappresentato.

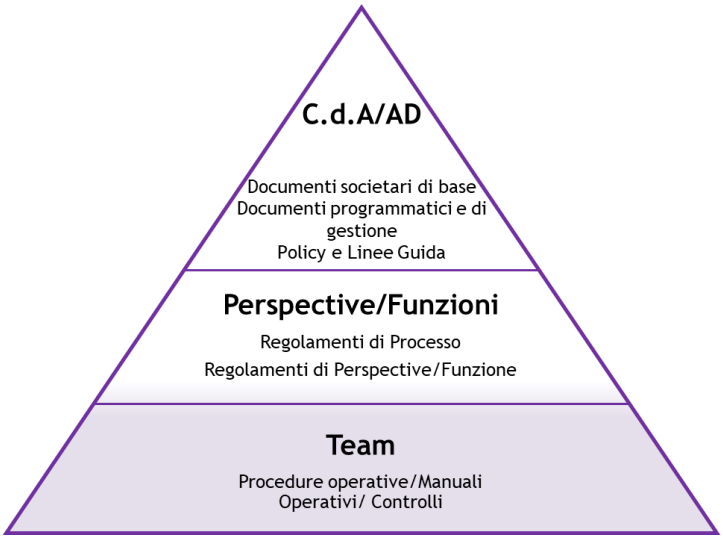


Figura 1: Modello della normativa interna di riferimento

3 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.

Per la gestione degli incidenti si prevede il coinvolgimento delle *Perspective* della Società, di opportune funzioni della Capogruppo Banca Mediolanum (che svolgono in *outsourcing* servizi aziendali in virtù di un apposito accordo di esternalizzazione) e delle strutture organizzative degli *outsourcer tecnologici*, che si impegnano, per quanto di competenza, ad applicare rigorosamente i principi contenuti nella *Policy di Incident Management di Flowe*.

Si prevede che l'evento possa essere segnalato da tutti i dipendenti, i fornitori esterni ed i clienti della Società. Il personale abilitato della *Perspective*, in qualità di *Incident 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.

In generale tutte le *Perspective* presidiano le attività del servizio erogato dagli *outsourcer* di propria competenza, definendo e aggiornando le metriche di controllo previste nei contratti.

A fronte di ogni anomalia rilevata con impatto sull'operatività di processo o di business, gli operatori di Flowe, coordinandosi con il proprio referente, censiscono l'evento sulle apposite piattaforme, come spiegato nel prosieguo del documento.

Vengono indicati di seguito i ruoli e le responsabilità dei principali attori coinvolti per la gestione degli *incidenti* in Flowe.

3.1 Incident Handler

L'*incident handler* è la persona all'interno di una Perspective owner del servizio/applicazione impattato dall'*incident* e ha la responsabilità di:

- ricevere tutte le segnalazioni relative agli incidenti che possono o potrebbero avere un impatto sull'operatività di business o di processo e avvia, con il supporto delle *Perspective* coinvolte, la raccolta dei dati necessari e alla relativa valutazione di impatto;
- gestire gli incidenti operativi o di sicurezza che impattano Flowe sia classificati come "*Minor*" che come "*Major*";
- analizzare e valutare ogni possibile evento configurabile come incidente al fine di determinarne la tipologia (operativo o *cyber*) e la gravità, sulla base dei dati raccolti e dei parametri di Banca d'Italia, coinvolgendo in modo tempestivo tutti gli attori interessati;
- attivare tempestivamente il Team IT Operation Security & Governance nel caso ci sia una valutazione di *incident* di tipo "*Major*";
- presidiare il processo di risoluzione dell'incidente garantendo, fino alla completa risoluzione dello stesso, un costante *follow-up* delle azioni intraprese e delle tempistiche di risoluzione ai clienti, alle Funzioni aziendali coinvolte, agli *outsourcer* e all'*Amministratore Delegato* della *Società*;
- tenere traccia di tutti gli *incident*i oggetto di valutazione e dell'esito dell'istruttoria. Per questa attività è stato individuato *Azure DevOps* come supporto a disposizione

sia alle funzioni interne a Flowe che ai soggetti esterni alla Società coinvolti nel processo;
- presidiare lo strumento di supporto per la registrazione e gestione degli *incident*i al fine di attivare tempestivamente le procedure di ripristino e verificare la correttezza delle informazioni registrate;
- monitorare costantemente la correttezza delle informazioni inserite all'interno del *tool Azure DevOps*;
- Identificare e tracciare, di concerto con gli opportuni interlocutori, la *root cause analysis* e *lesson learned* degli incidenti;
- archiviare le informazioni relative all'*incident* su *Azure DevOps* per quanto di propria competenza.

3.2 Incident Assignee

L'*incident assignee* è la persona che in un determinato momento ha in carico la gestione dell'*incident*. L'*incident assignee* può cambiare durante il processo di gestione dell'*incident*. Il cambio di assignee consente la collaborazione tra team differenti..

3.3 Focal point della perspective

Il focal point è la persona all'interno di una perspective che segnala un evento che potrebbe essere un incident. La segnalazione viene presa in carico all'incident handler che da il via al processo di gestione dell'incident.

3.4 IT Operation, Security & Governance

Il team IT Operation, Security & Governance ha la responsabilità di:

- effettuare un controllo di secondo livello sulla classificazione dell'incidente (major) effettuata dagli *Incident Handler*;
- verificare la fondatezza delle segnalazioni di eventuali *Data Breach* rilevati dalle *Perspective* e segnalarli all'Ufficio Privacy di Banca Mediolanum;
- segnalare, all'Unità di Supporto Manageriale Service Policy & Procedures, all'interno della *Direzione Service, Operations & ICT* di Banca Mediolanum gli *incident*i in tema PSD2 e al Settore IT Security di Banca Mediolanum gli *incident*i *cyber;*
- attivare il processo di classificazione e segnalazione descritto nella *Procedura operativa di classificazione e segnalazione degli incidenti* qualora le caratteristiche dell'incidente fossero tali da ipotizzarne una classificazione come *major incident*;

3.5 Team IT Monitoring

Il team IT Monitoring ha la responsabilità di:

- assicurare il monitoraggio della piattaforma applicativa di Flowe al fine di riscontrare eventuali incidenti e di aprire segnalazioni nel tool di *incident management*;
- assegnare l'*incident* all'*incident handler*;

3.6 Team Outsourcer Governance

Il team Outsourcer Governance ha la responsabilità di:

- gestire i ticket verso gli *outsourcer* coinvolti nel processo di *incident management*;
- raccogliere segnalazioni di *incident* da parte degli *outsourcers* e di segnalarli nel tool di *incident management*;
- verificare gli SLA contrattuali;
- accertarsi della risoluzione dell'*incident* da parte del fornitore;
- assicurarsi che il fornitore abbia fornito la *root cause analysis*;

3.7 Organization & Business Continuity

Organization & Business Continuity presidia tutti gli adempimenti ordinari e straordinari in tema di *business continuity*, in attuazione del piano di *Business Continuity* e in esecuzione degli indirizzi ricevuti dagli Organi Amministrativi e dalle Funzioni di Controllo.

3.8 Nell'ambito della presente procedura operativa, il Business Continuity Office 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 il Team IT Operation, Security & Governance la gravità dell'impatto dell'incidente.UNITÀ ORGANIZZATIVE DELLA CAPOGRUPPO

3.8.1 FUNZIONE RISK MANAGEMENT

La *Funzione 'Risk Management'* verifica, raccoglie e riconcilia, con il supporto delle altre *Perspective* di Flowe[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 e in conformità a quanto disciplinato dalla *Policy di Controllo e Gestione dei Rischi Operativi*.

3.8.2 UFFICIO PRIVACY DI BANCA MEDIOLANUM

L'*Ufficio Privacy di Banca Mediolanum* ingaggiato dal *Team 'IT Operation, Security & Governance'* laddove questo rilevi un possibile *data breach* 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);
- Nelle casistiche previste dalla normativa, predisporre i contenuti della 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 dai *data breach* è responsabile dell'identificazione delle azioni per contenere e/o

[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.

minimizzare i rischi per gli interessati e prevenirne la replica.

Al fine di mantenere il costante aggiornamento dello stato del *data breach* e di individuare eventuali ulteriori *data breach* che non sono stati considerati come tali, ha accesso, in sola lettura, al registro degli *incident*i definito su *Azure DevOps*.

3.8.3 UNITÀ DI SUPPORTO MANAGERIALE SERVICE POLICY & PROCEDURES, DI BANCA MEDIOLANUM (PER INCIDENTI IN TEMA PSD2) E SETTORE IT SECURITY DI BANCA MEDIOLANUM (PER INCIDENTI IN TEMA CYBER)

- supporta il Team IT Operation, Security & Governance nella gestione, nella corretta classificazione e nella valutazione delle potenziali conseguenze degli *incident* rilevanti per il proprio ambito di competenza;
- monitora lo stato di risoluzione dell'incidente e di ripristino dell'operatività.

3.9 FORNITORI ESTERNI

Gli *outsourcer* coinvolti nell'erogazione dei servizi di pagamento, con riferimento al loro ambito specifico, hanno la responsabilità di:

- segnalare tempestivamente alla *Perspective* di riferimento in Flowe, nel rispetto delle tempistiche definite negli *SLA* contrattuali concordati con la Società stessa, ogni incidente trasmettendo tutte le informazioni utili per la determinazione della gravità dell'evento;
- gestire le attività volte alla risoluzione dell'incidente e fornire aggiornamenti puntuali sullo stato dell'incidente in corso di risoluzione sino alla completa gestione e ripristino della normalità;
- fornire la reportistica al termine dell'*incident* alla *Perspective* di riferimento in Flowe.

4 DETTAGLI PROCEDURA INCIDENT MANAGEMENT

4.1 DEFINIZIONI

Termine, acronimo o abbreviazione	Definizione
Incidente **Incident**	Un'interruzione non pianificata di un servizio IT o una riduzione della qualità di un servizio IT (ad esempio malfunzionamenti applicativi, degrado delle performance, etc.)
Incidenti di Sicurezza Cyber	Incident causati da attività volontaria e malevola riguardanti l'accesso, l'uso, la divulgazione, l'interruzione, la modifica o la distruzione non autorizzata delle risorse del prestatore di servizi di pagamento o incidenti o incident che comunque producono, anche involontariamente, diffusione e/o alterazione di dati riservati della clientela e/o dell'intermediario.
Incident Operativi	Incident 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). La diffusione e/o l'alterazione involontaria (ad esempio, per errore umano o software) di dati riservati della clientela e/o dell'intermediario ricade nella categoria degli incidenti cyber.
Root Cause Analisys	Analisi tecnica e di processo utile alla determinazione della causa di/degli incident ICT
Data Breach	Una 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.
Azure Moitor	Soluzione di monitoraggio completa per la raccolta, l'analisi e la risposta ai dati di monitoraggio provenienti dai tuoi ambienti cloud e on-premises.
Lesson learned	Esperienze estratte da attività precedenti che dovrebbero essere considerate in modo attivo per le azioni future. In particolare, si tratta di conoscenze acquisite durante l'operatività di un servizio e che possono essere applicate alle fasi precedenti del ciclo di vita del servizio IT

4.2 PROCESSO

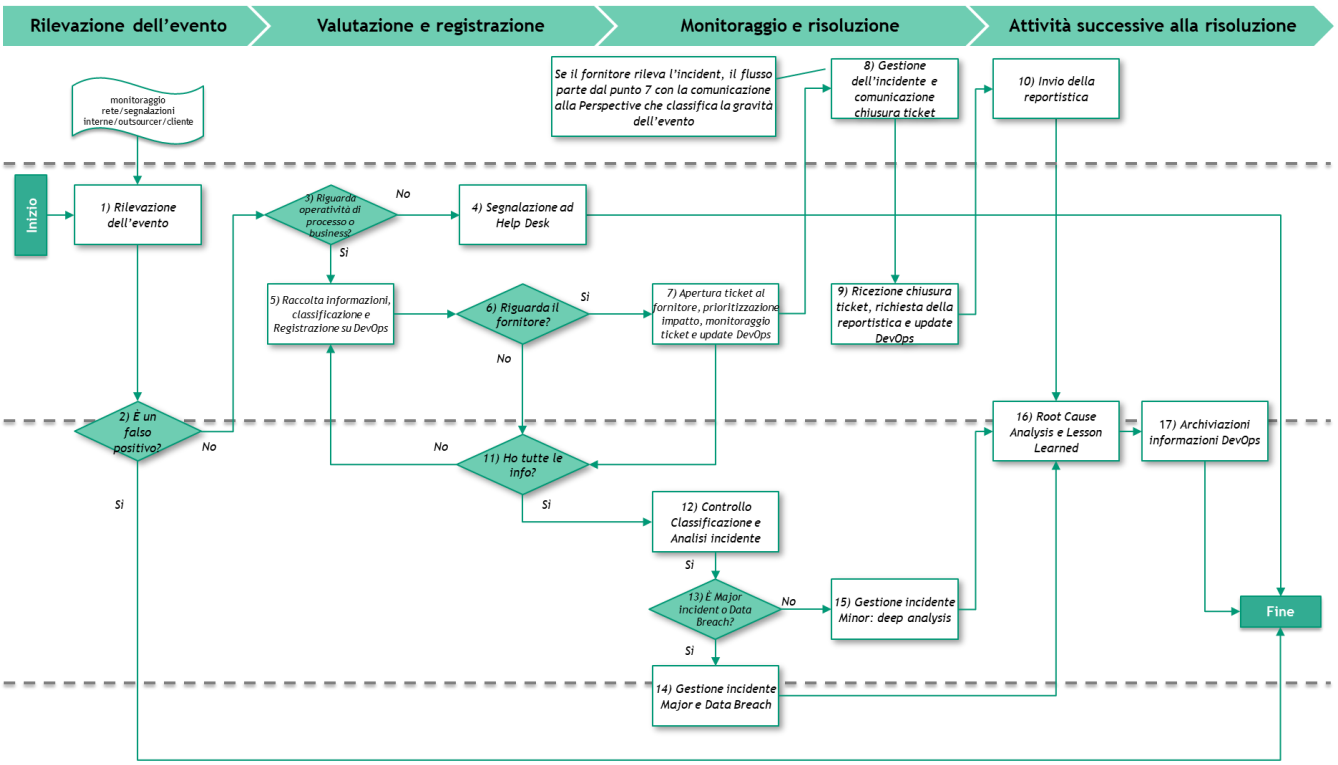
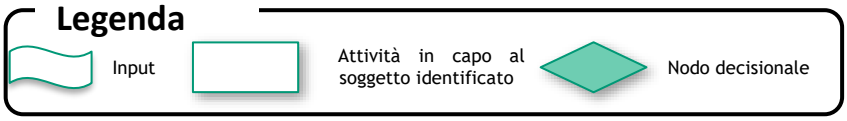


Figura 2: Flusso gestione incidenti



Di seguito sono descritte le attività operative del processo di gestione degli incidenti.

ID	NOME	DESCRIZIONE	ATTORE
1	**Rilevazione dell'evento**	Il flusso inizia con rilevazione degli eventi, la quale assume un ruolo cruciale nella gestione degli stessi, per tale ragione sono previsti diversi **canali di segnalazione**: • rilevazione mediante piattaforme/dashboard/log per il monitoraggio degli asset del sistema informativo e degli eventi esterni; • comunicazione da eventuali altre strutture della Società che possono rilevare un evento; • segnalazioni di terze parti (clienti, outsourcer) coinvolte a qualsiasi titolo dagli effetti e dall'impatto dell'evento.	Tutte le *Perspective* di Flowe Terze parti
2	**Verifica falso positivo**	L'*incident handler* constata se l'evento rilevato *Azure Monitor* sia un Falso positivo. In caso di falso positivo, il flusso termina in tale fase. In caso contrario, il flusso procede con la fase 3.	*Incident Handler*
3	**Riguarda operatività di processo o business?**	Il focal point valuta se l'evento impatta o potrebbe impattare l'operatività di processo o di business. Pertanto, tutti i casi che riguardano un problema tecnico, andranno segnalati all' Help Desk operativo di Flowe e il flusso continua al punto 4. A titolo esemplificativo e non esaustivo si riportano i casi che non devono essere censiti: • malfunzionamento posta elettronica (Outlook); • malfunzionamento Microsoft Teams; • impossibilità di accedere al sito Web del Portale aziendale; • impossibilità di effettuare aggiornamenti. In caso l'evento rientri nei casi che debbano essere censiti si prosegue con la fase 5.	*Focal point* della *Perspective* che ha rilevato l'evento

4	**Segnalazione ad Help Desk**	Il riscontro di un problema tecnico e, pertanto, non riguardante l'operatività di processo o di business, viene segnalato all'Help Desk mediante apposito tool di gestione ticket. Il flusso termina in tale fase.	*Focal point* della *Perspective* che ha rilevato l'evento
5	**Raccolta informazioni, classificazione e Registrazione su *DevOps***	A fronte di ogni evento rilevato che abbia o potrebbe avere un impatto sulla operatività di processo o di business della Società, l'incident handler ha la responsabilità di garantire la tracciatura nell'apposito database degli incident su Azure DevOps: • la classificazione dell'incidente, selezionando una delle opzioni disponibili (cyber, operativa), • la prioritàche deve essere data alla risoluzione dell'incident sulla base dei criteri elencati al par. 4.4; • una descrizione dettagliata del problema; • la data dell'apertura dell'*incident*; • l'area impattata, selezionando una delle opzioni disponibili; • l'indicazione che l'*incident* abbia avuto o avrà un impatto sui clienti; • la data di inizio dell'*incident*; • la dimensione dell'impatto in termini di numero di clienti coinvolti, selezionando una delle opzioni disponibili; • una indicazione della tipologia del danno, selezionando una delle opzioni disponibili; • l'indicazione che l'*incident* rappresenti un grave problema di sicurezza; • i sistemi IT eventualmente impattati, selezionando tutte quelle di interesse tra quelle disponibili; • l'eventuale riferimento del ticket assegnato dall'outsourcer all'*incident*; • gli outsourcer eventualmente impattati, selezionando tutti quelli di interesse tra quelli disponibili; • categoria di dati impattati dall'*incident*.	*Incident Handler* *Incident Assignee*
6	**Riguarda il fornitore?**	Dopo aver censito l'evento sulla piattaforma di *Azure DevOps*, l'*incident handler* verifica se l'evento impatta un'architettura esternalizzata. In tal caso il flusso procede con la fase 7, contrariamente con il punto 11.	*Incident Handler*

7	**Apertura ticket al fornitore, prioritizzazione impatto, monitoraggio ticket e update Devops**	L'incident assignee apre il ticket nei confronti del fornitore al fine di segnalare l'evento. L'evento dovrebbe essere prioritizzato sulla base dell'impatto che potrebbe avere sulla Società, come indicato al paragrafo 4.3 della presente Procedura. Quando l'incident assignee censisce l'evento sulla piattaforma del fornitore, indica, almeno: • la durata dell'evento; • il numero di clienti impattati; • se sono interessate le transazioni, qual è il numero di transazioni impattate e l'importo economico di quest'ultime. L'incident assignee che ha segnalato l'evento al fornitore è responsabile di verificare che quest'ultimo rispetti quanto previsto dagli SLA contrattuali. Spetta all'outsourcer governance assicurarsi che l'incidente venga gestito nei tempi previsti. Parallelamente, l'incident assignee si assicura di censire su *Azure DevOps* gli update relativi alla gestione del ticket.	*Outsorcer Governance* *Incident Assignee*
8	**Gestione dell'incidente e comunicazione chiusura ticket**	Il fornitore prende in carico l'incidente e lo gestisce rispettando quanto previsto negli accordi contrattuali. Al termine, comunica all'incident assignee che ha segnalato l'evento la chiusura dell'*incident* e la risoluzione dello stesso. Parallelamente, l'incident assigneesi assicura di censire su *Azure DevOps* gli update relativi alla gestione del ticket. Nel caso in cui il fornitore stesso si accorga della presenza di un *incident* sul proprio servizio erogato alla Società, esso comunica tempestivamente e in linea con quanto previsto dagli SLA contrattuali alla *Perspective* di riferimento l'*incident* al fine che essa possa adeguatamente censirlo.	Fornitore servizio esternalizzato
9	**Ricezione chiusura ticket e richiesta della reportistica e Update Devops**	L' *Outsorcer Governance* accerta la chiusura dell'*incident* e richiede quando necessario al fornitore la documentazione utile a consentire l'analisi delle attività in ottica *lesson learned*. Parallelamente, l'incident assignee censisce su *Azure DevOps* la chiusura dell'*incident*.	*Outsorcer Governance* *Incident Assignee*

10	**Invio della reportistica**	Il fornitore, al seguito della chiusura dell'*incident* invia la reportistica richiesta alla Società. Tale reportistica deve essere analizzata dal *Team Outsourcer Governance*. Il flusso riprende al punto 16.	Fornitore servizio esternalizzato
11	**Verifica delle informazioni**	L'*incident handler* verifica che siano state inserite su Azure DevOps tutte le informazioni necessarie per poter classificare l'evento. In caso siano presenti, il flusso continua al punto 12, contrariamente si ritorna alla fase 5.	*Incident Handler*
12	**Controllo Classificazione e Analisi incidente**	Il Team IT Operation, Security & Governance in collaborazione con le altre unità organizzative e come meglio dettagliato dalla "*Procedura Operativa di classificazione e segnalazione degli incidenti*" di Flowe verifica la corretta classificazione dell'*incident* e lo analizza. Il *Team* verifica se vi siano le condizioni per attivare il processo per la segnalazione dell'*incident* all'Autorità di Vigilanza.	*Team IT Operation, Security & Governance*
13	**Verifica Major Incident o Data Breach**	Lo stesso *Team IT Operation, Security & Governance* potrebbe stabilire, dalle caratteristiche dello stesso rilevate dal registro su *Azure DevOps,* che ricorrano le condizioni per l'attivazione della procedura di gestione dei *major incident*. Inoltre, tale Team verifica se ci siano le condizioni per cui si possa trattare di un *data breach*. In caso affermativo di almeno una delle due alternative, il flusso procede alla fase 14, contrariamente con il punto 15.	*Team IT Operation, Security & Governance*

14	**Gestione incidente Major e Data Breach**	Nel caso in cui sussistano le condizioni per cui vi sia un Major incident e/o un data breach, il Team IT Operation, Security & Governan contatta le opportune strutture della Capogruppo, come meglio dettagliato dalla "*Procedura Operativa di classificazione e segnalazione degli incidenti*". Il Team IT Operation, Security & Governance segnala , nel più breve tempo possibile, il *data breach* all'*Ufficio Privacy di Banca Mediolanum* attraverso l'invio di una *email* alla casella di posta elettronica dedicata (segnalazionigdpr@mediolanum.it) in cui, se possibile, allega il «Modulo Di Raccolta Della Segnalazione», così da indirizzare correttamente le attività di identificazione del *data breach* e di effettuare le verifiche preliminari. Il Team IT Operation, Security & Governance a valle della rilevazione di un incidente Major, ingaggia *l'Unità di Supporto Manageriale Service Policy & Procedures* di Banca Mediolanum (per incidenti in ambito PSD2), il Settore *IT Security* di Banca Mediolanum (per incidenti in tema *cyber*), *e* Organization & Business Continuity in caso di incidente il cui impatto possa attivare potenzialmente uno degli scenari di continuità operativa, come meglio dettagliato dalla "*Procedura Operativa di classificazione e segnalazione degli incidenti*".	*Team IT Operation, Security & Governance* *Ufficio Privacy di Banca Mediolanum* *Unità di Supporto Manageriale Service Policy & Procedures* di Banca Mediolanum (per incidenti in ambito PSD2) Settore *IT Security* di Banca Mediolanum (per incidenti in tema *cyber*) Organization & Business Continuity *(impatti su Continuità Operativa)*
15	**Gestione incidente Minor: Deep Analysis**	Nel caso in cui il Team IT Operation, Security & Governanceil Team IT Operation, Security & Governance abbia valutato che non si tratti di un incidente *Major*, l'*incident handler* procede ad implementare le azioni di contrasto atte a mitigare le compromissioni della sicurezza derivanti da un incidente Minor operativo o di sicurezza. Il *Team* procede con una Deep Analysis *dell'incident* verificando la presenza di soluzioni a quest'ultimo: • nella *Knowledge Base*; • nell'elenco degli errori noti; • nei registri degli incidenti precedenti ed esistenti.	*Incident Handler*
16	**Root Cause Analysis e Lesson Learned**	A fronte di un incidente, l'*incident handler* raccoglie ed analizza le evidenze prodotte nella fase di gestione, al fine di identificare eventuali azioni di miglioramento. In particolare, sono agite le seguenti attività:	*Incident Handler*

		• **raccolta, inventariazione** e corretta **conservazione** delle **evidenze** scaturite dalla gestione degli eventi al fine di poter essere analizzate ed anche utilizzabili in caso di contenziosi;
		• **analisi dell'evento** finalizzato all'individuazione delle **azioni di rimedio:**
		  ○ definizione di adeguate procedure per l'analisi dei log di eventi e incidenti;
		  ○ utilizzo di copie delle **evidenze** raccolte durante la fase di gestione degli incidenti per lo svolgimento delle attività di analisi a posteriori preservando in tal modo l'integrità delle evidenze originali;
		  ○ contestualizzazione del processo di analisi dei dati di tracciamento in un'ottica di prevenzione volta all'individuazione di contromisure efficaci per i problemi riscontrati;
		  ○ **analisi degli incidenti** più ricorrenti quantificando e monitorando tipi, volumi e impatti al fine di definire e pianificare le opportune azioni correttive anche per migliorare la capacità di prevenzione;
		  ○ predisposizione di strumenti di **analisi a posteriori** basati su criteri logici che consentano l'esecuzione delle operazioni di ricerca, selezione e ordinamento dei dati raccolti;
		• in caso di incidenti che necessitano dell'**analisi forense**, deve essere:
		  ○ predisposta un'adeguata metodologia;
		  ○ prodotta copia dei supporti di memorizzazione da analizzare che garantisca la validità probatoria del supporto originale;
		• **Identificazioni Lesson Learned:** aggiornamento delle procedure operative di risposta agli incidenti e gli scenari di test con le informazioni, i canali e le tecniche utilizzate durante la gestione dell'incidente in modo da migliorare le azioni preventive adottate e dunque prevenire il verificarsi di nuovi incidenti similari o di potenziali crisi.	

17	**Archiviazione delle informazioni**	Il processo di gestione degli incidenti si conclude tracciando le attività svolte, archiviando le evidenze prodotte e producendo la reportistica di interesse. L'*incident handler*:	*Incident Handler*

		• effettua il tracciamento e l'archiviazione delle evidenze prodotte dalla gestione dell'evento; • effettua il tracciamento e l'archiviazione delle evidenze prodotte dalla gestione delle azioni di rimedio; • produce la reportistica relativa alle analisi a posteriori dell'evento; • produce la reportistica relativa alla gestione delle azioni di rimedio. Il flusso termina in tale fase.	

4.3 RILEVAZIONE

Flowe segue le indicazioni date da Banca d'Italia per identificare un *incident* intendendo con questo "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" (ad esempio, frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi).
L'identificazione di un incidente in Flowe può avvenire tramite:

- il monitoraggio dell'intera infrastruttura svolto dal *Team IT Monitoring* tramite *dashboard* dedicate, strumenti di rilevazione etc.
- Il *Team IT Operation, Security & Governance* intercetta, *alert* di sicurezza con il supporto di *dashboard/log* dedicate;
- la *Perspective Banking Services & Controls* a fronte di anomalie segnalate dalla clientela o dagli *outsourcer* valuta se ricorrano le circostanze di un possibile incidente da segnalare e l'eventuale riscontro da fornire al cliente o all'*outsourcer* che ha effettuato la segnalazione;
- i dipendenti Flowe di qualsiasi *Perspective*.

Tali *incident* possono includere, a titolo esemplificativo[3]:

- accessi logici o fisici non autorizzati a sistemi informatici o a dati;
- interruzioni prolungate di servizio non previste o pianificate;
- indisponibilità di un servizio o sistema o grave degrado delle prestazioni a seguito di attacco dall'esterno (negazione del servizio o *DoS*);
- utilizzo abusivo di un sistema per l'elaborazione o la conservazione di dati;
- modifica non autorizzata delle caratteristiche *hardware, firmware* e *software* di un dispositivo *ICT*;
- alterazioni della disponibilità, integrità e riservatezza di sistemi e dati a seguito di gravi malfunzionamenti che pregiudicano i livelli di servizio attesi;

[3] Fonte: Istruzioni per la segnalazione dei gravi incidenti operativi o di sicurezza – IP, IMEL, succursali di banche extracomunitarie aventi sede negli stati indicati nell'allegato a delle disposizioni introduttive della circ. 285

- compromissione di reti di comunicazione a livello locale o geografico;
- alterazione volontaria del codice sorgente di applicativi al fine di aggirare controlli, effettuare accessi non autorizzati a sistemi e dati o arrecare danni all'interno o all'esterno dell'azienda;
- frodi perpetrate attraverso strumenti informatici o tecniche di *social engineering*;
- diffusione, volontaria o involontaria, di dati riservati o sensibili;
- alterazione dei *file* di *log* o delle tracce di *audit*.

Si precisa che nella definizione di "incidente operativo o di sicurezza" sono escluse le indisponibilità programmate, ma sono compresi:

- gli eventi che non derivano da un malfunzionamento IT che hanno impatto negativo rilevante sui clienti fruitori di servizi di pagamento;
- gli eventi fraudolenti (c.d. «frodi») quali transazioni di pagamento:
  - non autorizzate;
  - eseguite o autorizzate da un pagatore che ha agito in modo disonesto o ingannevole;
  - effettuate mediante manipolazione del pagatore.

4.4 CLASSIFICAZIONE DELL'INCIDENTE

Il processo di *Incident Management* recepisce in input tutti gli incidenti segnalati dagli utenti e dalle procedure automatiche di controllo del funzionamento del sistema informativo.

Gli incidenti sono categorizzati in base alla priorità che viene determinata dalla combinazione di impatto e da un valore di urgenza attribuito al sistema informativo coinvolto.

L'impatto indica la diffusione dell'evento e può assumere i seguenti quattro valori:

1. **Vasto/diffuso**:
   a. Applicazione/servizio completamente indisponibile per più utenti (fermo totale di un servizio/applicazione)
   b. Anomalia applicativa *rilevante*, ovvero che pregiudica totalmente la normale operatività dei relativi utenti e, pertanto, l'operatività di processo o di business
   c. Alterazioni o altre anomalie sui dati relativi a gran parte degli utenti del servizio
   d. Furto o diffusione (anche potenziali) di gran parte delle informazioni gestite dal servizio/applicazione
   e. Frodi indirizzate verso gran parte degli utenti dell'applicazione/servizio

2. **Significativo/grande**:
   a. Applicazione/servizio degradato per più utenti
   b. Errore bloccante, con impatto su un numero significativo di utenti, per la soluzione del quale esistono soluzioni alternative
   c. Anomalia applicativa significativa, ovvero che non pregiudica totalmente la normale operatività, ma che non permette l'erogazione corretta di una o più funzionalità di primaria importanza
   d. Alterazioni o altre anomalie sui dati relativi ad un numero limitato di utenti

(i.e. inferiore al 10%)

e. Furto o diffusione (anche potenziali) di un numero limitato delle informazioni gestite dal servizio / applicazione
f. Frodi indirizzate verso un numero limitato di utenti dell'applicazione/ servizio

3. **Moderato/limitato**:
   a. Applicazione/servizio completamente indisponibile per un singolo utente
   b. Operatività di processo o di business bloccata per un singolo utente
   c. Anomalia applicativa moderata, ovvero che non pregiudica la normale operatività, ma che non consente la fruizione di una o più funzionalità di secondaria importanza
   d. Alterazioni o altre anomalie sui dati relativi a un singolo utente

4. **Minimo/Localizzato**:
   a. Nessun degrado significativo o un degrado solo per un singolo utente
   b. Operatività garantita
   c. Anomalia applicativa lieve, ovvero non critica per l'operatività dell'utente

L'urgenza rappresenta un valore predeterminato in funzione del livello di gravità rilevato:

1. **Critica**
2. **Alta**
3. **Media**
4. **Bassa**

La **priorità** è un parametro calcolato sulla base dell'impatto e dell'urgenza secondo la matrice di seguito riportata.

PRIORITÀ INCIDENT		URGENZA			
		1 – Critica	2- Alta	3- Media	4- Bassa
IMPATTO	1- Vasto/diffuso	CRITICA	CRITICA	ALTA	BASSA
	2 - Significativo/Grande	CRITICA	ALTA	MEDIA	BASSA
	3 - Moderato/limitato	ALTA	ALTA	MEDIA	BASSA
	4 - Minimo/localizzato	ALTA	MEDIA	MEDIA	BASSA

4.5 REGISTRAZIONE DELL'INCIDENTE

Devono essere registrati tutti gli incidenti informatici che potrebbero rappresentare una minaccia per l'operatività di processo o il business della Società. L'incident handler che registra l'incidente deve seguire i criteri di classificazione descritti al precedente paragrafo.

Non devono essere censiti tutti gli eventi riguardanti un malfunzionamento tecnico ad esempio della postazione di lavoro e che, pertanto, possono essere risolti contattando l'Help Desk.

Ogni volta che si verifica un incidente che impatta o potrebbe impattare l'operatività di processo o di business, l'incident incident handler/assignee deve censirlo sulla piattaforma di *Azure DevOps*. Nel caso in cui l'incidente riguardi un servizio esternalizzato, l'incident handler/assignee deve censirlo anche sulla piattaforma del fornitore. A titolo esemplificativo e non esaustivo si riporta un elenco dei servizi esternalizzati:

- *Onboarding*;
- Gestione pagamenti,
- *Core banking*;
- Bonifici;
- Gestione carte.

Quando l'incident handler/assignee censisce l'incidente sulla piattaforma del fornitore, indica, almeno:

- la durata dell'evento;
- il numero di clienti impattati;
- se sono interessate le transazioni, qual è il numero di transazioni impattate e l'importo economico di quest'ultime.

4.6 SEGNALAZIONE ED ESCALATION

Una volta censito l'*incident*, se necessario, l'*incident handler segnala* al *Team IT Operation, Security & Governance* che effettua un controllo di secondo livello sulla classificazione dell'incidente e procede ad analizzarlo. L'*ownership* dell'*incident* rimane in carico all'incident handler che ne ha effettuato il censimento.

Il Team IT Operation, Security & Governance in caso di incidente Major o di Data Breach procede al coinvolgimento della Capogruppo come descritto nella *Procedura Operativa di classificazione e segnalazione degli incidenti*.

In caso di *incident* che non richiede l'escalation alla Capogruppo e che non riguarda i servizi esternalizzati, la risoluzione dello stesso è in capo all'incident handler.

4.7 GESTIONE E CHIUSURA DELL'INCIDENT

L'incident handler nel corso della gestione dell'*incident* aggiorna costantemente tutte le informazioni inserite in origine e documenta le azioni intraprese nel campo *Descrizione Risoluzione* sino alla completa chiusura dell'*incident*.

A *incident* concluso compila i campi:

- *Data fine incidente*
- *Data chiusura* incidente

E modifica lo *Stato* dell'*incident* in "chiuso".

Nel caso in cui l'*incident* abbia impattato un servizio esternalizzato, è in capo al team Outsourcer Governance di assicurarsi che quest'ultimo rispetti quanto previsto dagli SLA contrattuali in merito alla gestione e risoluzione dell'*incident*.

4.8 ATTIVITÀ SUCCESSIVE ALLA RISOLUZIONE

Alla risoluzione dell'incident, *l'incident handler* deve effettuare la *root cause analysis*, identificando le cause che hanno portato al verificarsi dell'*incident*.

Le *lesson learned* apprese da queste analisi dovrebbero essere incorporate nelle attività di gestione degli incidenti, nelle procedure di risposta agli incidenti, nell'*incident response plan* e nella formazione del personale.

Se l'incidente ha riguardato un servizio esternalizzato, alla chiusura dell'*incident* il fornitore deve inviare la documentazione adeguata a consentire all'*incident handler* di effettuare la *root cause analysis*,

È in capo all'incident handler verificare l'adeguata archiviazione delle informazioni.

5 INCIDENT RESPONSE PLAN

Il seguente paragrafo intende rappresentare alcuni degli scenari che potrebbero verificarsi sulla Società.

5.1 SCENARIO 1: EVENTO CHE IMPATTA UN SERVIZIO ESTERNALIZZATO

ID	NOME	DESCRIZIONE	ATTORE
1	**Rilevazione dell'evento**	Il flusso inizia con la segnalazione del cliente in quanto non riesce accedere al proprio conto bancario ed eseguire operazioni, ad esempio, i bonifici.	Flowe
3	**Riguarda operatività di processo o business?**	L'incident handler constata che il problema segnalato dal cliente potrebbe impattare l'operatività di processo o di business, pertanto decide di segnalare tale evento aprendo un ticket su *Azure DevOps*.	*Incident Handler*

5	**Raccolta informazioni, classificazione e Registrazione su *DevOps***	A questo punto, l' incident handler/assignee procede con il censimento dell'incidente su *Azure DevOps* nell'apposito database degli *incident* indicando: • la classificazione dell'incidente, selezionando una delle opzioni disponibili (*cyber*, operativo); • l'impatto che l'*incident* ha determinato o potrebbe determinare, selezionando una delle opzioni disponibili, sulla base dei criteri sopra elencati; • una descrizione dettagliata del problema; • la data dell'apertura dell'*incident*; • l'area impattata, selezionando una delle opzioni • disponibili; • l'indicazione che l'incident abbia avuto o avrà un impatto sui clienti; • la data di inizio dell'incident; • la dimensione dell'impatto in termini di numero di clienti coinvolti, selezionando una delle opzioni disponibili; • una indicazione della tipologia del danno, selezionando una delle opzioni disponibili; • l'indicazione che l'incident rappresenti un grave problema di sicurezza; • i sistemi IT eventualmente impattati, selezionando tutte quelle di interesse tra quelle disponibili; • l'eventuale riferimento del ticket assegnato dall'outsourcer all'incident; • gli outsourcer eventualmente impattati, selezionando tutti quelle di interesse tra quelli disponibili; • categoria di dati impattati dall'incident.	*Incident Handler* *Incident Assignee*
6	**Riguarda il fornitore?**	Dopo aver censito l'evento sulla piattaforma di *Azure DevOps*, l'incident assignee verifica se l'incidente impatta un'architettura esternalizzata. Dato che il core banking riguarda un'attività esternalizzata , l'incident assignee apre il ticket nei confronti del fornitore.	*Outsourcer Govenrnance* *Incident Assignee*
7	**Apertura ticket al fornitore, prioritizzazione impatto, monitoraggio ticket e update Devops**	L'incident assignee di Flowe incaricato apre il ticket nei confronti del fornitore al fine di segnalare l'*incident*. Quest'ultimo dovrebbe essere prioritizzato sulla base dell'impatto che potrebbe avere sulla Società, come spiegato al paragrafo 4.3 della presente Procedura. L' incident assignee che ha segnalato l'*incident* al fornitore è responsabile di verificare che quest'ultimo rispetti quanto previsto dagli SLA contrattuali. Inoltre, spetta all' incident assignee assicurarsi che l'incidente venga gestito nei tempi previsti.	*Outsourcer Govenrnance* *Incident Assignee*

		Parallelamente, l' incident assignee si assicura di censire su *Azure DevOps* gli update relativi alla gestione del ticket.	
8	**Gestione dell'incidente e comunicazione chiusura ticket**	Temenos prende in carico l'incidente e lo gestisce rispettando quanto previsto negli accordi contrattuali. Al termine, comunica all' incident assignee che ha segnalato l'*incident* la chiusura e la risoluzione dello stesso.	Temenos
9	**Ricezione chiusura ticket e richiesta della reportistica e Update Devops**	L'outsourcer governance accerta la chiusura dell'*incident* e richiede al fornitore la documentazione necessaria a consentire l'analisi delle attività in ottica *lesson learned*. Parallelamente, l'incident assignee censisce su Azure DevOps la chiusura dell'*incident*.	*Outsourcer Govenrnance* *Incident Assignee*
10	**Invio della reportistica**	Temenos, al seguito della chiusura dell'*incident* invia la reportistica richiesta alla Società. Tale reportistica deve essere analizzata dal *Team IT Operation, Security & Governance* in collaborazione con la *Perspective* che ha rilevato l'evento. Il flusso riprende al punto 16.	Temenos
11	**Verifica delle informazioni**	L'incident handler verifica che siano state inserite su *Azure DevOps* tutte le informazioni necessarie per poter classificare l'evento. In caso siano presenti, il flusso continua al punto 12, contrariamente si ritorna alla fase 4.	*Incident Handler*
12	**Controllo Classificazione e Analisi incidente**	Il Team IT Operation, Security & Governance in collaborazione con le altre unità organizzative e come meglio dettagliato dalla "*Procedura Operativa di classificazione e segnalazione degli incidenti*" di Flowe verifica la corretta classificazione dell'*incident* e lo analizza. Il *Team* verifica se vi siano le condizioni per attivare il processo per la segnalazione dell'*incident* all'Autorità di Vigilanza.	*Team IT Operation, Security & Governance*
13	**Verifica *Major Incident* o *Data Breach***	Lo stesso *Team IT Operation, Security & Governance* potrebbe stabilire che ricorrano le condizioni per l'attivazione della procedura di gestione dei *major incident* dalle caratteristiche dello stesso rilevate dal registro su *Azure DevOps*. Inoltre, tale Team verifica se si verificano le condizioni per cui si possa trattare di un *data breach*.	*Team IT Operation, Security & Governance*

		In caso affermativo di almeno una delle due alternative, il flusso procede alla fase 14, contrariamente con il punto 15.	
14	**Gestione incidente major e Data Breach**	Nel caso in cui sussistano le condizioni per cui vi sia un *Major incident* e/o un *data breach*, il Team IT Operation, Security & Governance contatta le opportune strutture della Capogruppo, come meglio dettagliato dalla "*Procedura Operativa di classificazione e segnalazione degli incidenti*". Il Team IT Operation, Security & Governance segnala , nel più breve tempo possibile, il data breach all'*Ufficio Privacy di Banca Mediolanum* attraverso l'invio di una *email* alla casella di posta elettronica dedicata (segnalazionigdpr@mediolanum.it) cui, se possibile, allega il «Modulo Di Raccolta Della Segnalazione», così da indirizzare correttamente le attività di identificazione del *data breach* e di effettuare le verifiche preliminari. Il Team IT Operation, Security & Governance a valle della rilevazione di un incidente Major, ingaggia *l'Unità di Supporto Manageriale Service Policy & Procedures* di Banca Mediolanum (per incidenti in ambito PSD2), l'*Unità IT Security* di Banca Mediolanum (per incidenti in tema *cyber*), *e* Organization & Business Continuity in caso di incidente il cui impatto possa attivare potenzialmente uno degli scenari di continuità operativa, come meglio dettagliato dalla "*Procedura Operativa di classificazione e segnalazione degli incidenti*".	*Team IT Operation, Security & Governance Ufficio Privacy di Banca Mediolanum* *Unità di Supporto Manageriale Service Policy & Procedures* di Banca Mediolanum (per incidenti in ambito PSD2) l'*Unità IT Security* di Banca Mediolanum (per incidenti in tema *cyber*) Organization & Business Continuity *(impatti su Continuità Operativa)*
15	**Gestione incidente Minor: Deep Analysis**	Nel caso in cui il Team IT Operation, Security & Governance abbia valutato che non si tratti di un incidente Major, l'incident handler procede ad implementare le azioni di contrasto atte a mitigare le compromissioni della sicurezza derivanti da un incidente operativo o di sicurezza Minor. Il *Team* procede con una Deep Analysis *dell'incident* verificando la presenza di soluzioni a quest'ultimo: • nella Knowledge Base; • nell'elenco degli errori noti; • nei registri degli incidenti precedenti ed esistenti.	*Incident Hahdler*

16	**Root Cause Analysis e Lesson Learned**	A fronte di un incidente, l'incident handler raccoglie ed analizza le evidenze prodotte nella fase di gestione, al fine di identificare eventuali azioni di miglioramento. In particolare, sono agite le seguenti attività: • **raccolta, inventariazione** e corretta **conservazione** delle **evidenze** scaturite dalla gestione degli incidenti al fine di poter essere analizzate ed anche utilizzabili in caso di contenziosi; • **analisi dell'incidente** finalizzato all'individuazione delle **azioni di rimedio:** o definizione di adeguate procedure per l'analisi dei log di eventi e incidenti; o utilizzo di copie delle **evidenze** raccolte durante la fase di gestione degli incidenti per lo svolgimento delle attività di analisi a posteriori preservando in tal modo l'integrità delle evidenze originali; o contestualizzazione del processo di analisi dei dati di tracciamento in un'ottica di prevenzione volta all'individuazione di contromisure efficaci per i problemi riscontrati; o **analisi degli incidenti** più ricorrenti quantificando e monitorando tipi, volumi e impatti al fine di definire e pianificare le opportune azioni correttive anche per migliorare la capacità di prevenzione; o predisposizione di strumenti di **analisi a posteriori** basati su criteri logici che consentano l'esecuzione delle operazioni di ricerca, selezione e ordinamento dei dati raccolti; • in caso di incidenti che necessitano dell'**analisi forense**, deve essere: o predisposta un'adeguata metodologia; o prodotta copia dei supporti di memorizzazione da analizzare che garantisca la validità probatoria del supporto originale; • **Identificazioni Lesson Learned:** aggiornamento delle procedure operative di risposta agli incidenti e gli scenari di test con le informazioni, i canali e le tecniche utilizzate durante la gestione dell'incidente in modo da migliorare le azioni preventive adottate e dunque prevenire il verificarsi di nuovi incidenti similari o di potenziali crisi.	*Incident Handler*

17	**Archiviazione delle informazioni**	Il processo di gestione degli incidenti si conclude tracciando le attività svolta, archiviando le evidenze prodotte e producendo la reportistica di interesse. In particolare l'*incident handler*: • effettua il tracciamento e l'archiviazione delle evidenze prodotte dalla gestione dell'evento; • effettua il tracciamento e l'archiviazione delle evidenze prodotte dalla gestione delle azioni di rimedio; • produce la reportistica relativa alle analisi a posteriori dell'evento; • produce la reportistica relativa alla gestione delle azioni di rimedio. Il flusso termina in tale fase.	*Incident Handler*

5.2 SCENARIO 2: EVENTO CHE IMPATTA UN SERVIZIO NON ESTERNALIZZATO

ID	NOME	DESCRIZIONE	ATTORE
1	**Rilevazione dell'evento**	Il flusso inizia con la segnalazione da parte di IT Monitoring in quanto tramite *Azure Monitor* è stato rilevato un evento con livello di Severity (0,1, o 2) su un'architettura Flowe.	IT Monitoring
2	**Verifica Falso positivo**	L'*incident handler* constata se l'evento rilevato tramite Azure Monitor sia un Falso positivo. In caso di falso positivo, il flusso termina in tale fase. In caso contrario, il flusso procede con la fase 3.	*Incident Handler*
3	**Riguarda operatività di processo o business?**	L'incident handler constata che il problema segnalato potrebbe impattare l'operatività di processo o di business, pertanto decide di segnalare tale evento aprendo un ticket su *Azure DevOps*.	*Incident Handler*
5	**Raccolta informazioni, classificazione e Registrazione su *DevOps***	A questo punto, l'incident handler/assignee procede con il censimento dell'incidente su *Azure DevOps* nell'apposito database degli *incident* indicando: • la classificazione dell'incidente, selezionando una delle opzioni disponibili (*cyber*, *operativa*);	*Incident Handler* *Incident Assignee*

		• l'impatto che l'incident ha determinato o potrebbe determinare, selezionando una delle opzioni disponibili, sulla base dei criteri sopra elencati; • una descrizione dettagliata del problema; • la data dell'apertura dell'*incident*; • l'area impattata, selezionando una delle opzioni • disponibili; • l'indicazione che l'incident abbia avuto o avrà un impatto sui clienti; • la data di inizio dell'incident; • la dimensione dell'impatto in termini di numero di clienti coinvolti, selezionando una delle opzioni disponibili; • una indicazione della tipologia del danno, selezionando una delle opzioni disponibili; • l'indicazione che l'incident rappresenti un grave problema di sicurezza; • i sistemi IT eventualmente impattati, selezionando tutte quelle di interesse tra quelle disponibili; • l'eventuale riferimento del ticket assegnato dall'outsourcer all'incident; • gli outsourcer eventualmente impattati, selezionando tutti quelle di interesse tra quelli disponibili; • categoria di dati impattati dall'incident.	
6	**Riguarda il fornitore?**	Dopo aver censito l'*incident* sulla piattaforma di *Azure DevOps*, l'incident handler verifica se l'incidente impatta un'architettura esternalizzata. Dato che in questo caso si tratta di un'architettura interna, non apre nessun ticket nei confronti dei fornitori.	*Incident Handler*
11	**Verifica delle informazioni**	L'incident handler verifica che siano state inserite su *Azure DevOps* tutte le informazioni necessarie per poter classificare l'evento. In caso siano presenti, il flusso continua al punto 11, contrariamente si ritorna alla fase 4.	*Incident Handler*
12	**Controllo Classificazione e Analisi incidente**	Il Team IT Operation, Security & Governance in collaborazione con le altre unità organizzative e come meglio dettagliato dalla "*Procedura Operativa di classificazione e segnalazione degli incidenti*" di Flowe verifica la corretta classificazione dell'*incident* e lo analizza. Il *Team* verifica se vi siano le condizioni per	*Team IT Operation, Security & Governance*

		attivare il processo per la segnalazione dell'*incident* all'Autorità di Vigilanza.	
13	**Verifica Major Incident o Data Breach**	Lo stesso *Team IT Operation, Security & Governance* potrebbe stabilire che ricorrano le condizioni per l'attivazione della procedura di gestione dei *major incident* dalle caratteristiche dello stesso rilevate dal registro su *Azure DevOps*. Inoltre, tale Team verifica se ci siano le condizioni per cui si possa trattare di un data breach. In caso affermativo di almeno una delle due alternative, il flusso procede alla fase 12, contrariamente con il punto 13.	*Team IT Operation, Security & Governance*
14	**Gestione incidente major e Data Breach**	Nel caso in cui sussistano le condizioni per cui vi sia un Major incident e/o un data breach, il Team IT Operation, Security & Governance contatta le opportune strutture della Capogruppo, come meglio dettagliato dalla "*Procedura Operativa di classificazione e segnalazione degli incidenti*". Il Team IT Operation, Security & Governance segnala , nel più breve tempo possibile, il data breach all'*Ufficio Privacy di Banca Mediolanum* attraverso l'invio di una *email* alla casella di posta elettronica dedicata (segnalazionigdpr@mediolanum.it) cui, se possibile, allega il «Modulo Di Raccolta Della Segnalazione», così da indirizzare correttamente le attività di identificazione del *data breach* e di effettuare le verifiche preliminari. Il Team IT Operation, Security & Governance a valle della rilevazione di un incidente Major, ingaggia *l'Unità di Supporto Manageriale Service Policy & Procedures* di Banca Mediolanum (per incidenti in ambito PSD2), l'*Unità IT Security* di Banca Mediolanum (per incidenti in tema *cyber*), *e* Organization & Business Continuity in caso di incidente il cui impatto possa attivare potenzialmente uno degli scenari di continuità operativa, come meglio dettagliato dalla "*Procedura Operativa di classificazione e segnalazione degli incidenti*".	*Team IT Operation, Security & Governance* *Ufficio Privacy di Banca Mediolanum* *Unità di Supporto Manageriale Service Policy & Procedures* di Banca Mediolanum (per incidenti in ambito PSD2) l'*Unità IT Security* di Banca Mediolanum (per incidenti in tema *cyber*) Organization & Business Continuity *(impatti su Continuità Operativa)*
15	**Gestione incidente**	Nel caso in cui il Team IT Operation, Security & Governance abbia valutato che non si tratti di un incidente Major, l'incident handler procede ad implementare le azioni di contrasto atte a mitigare le	*Incident Handler*

	Minor: Deep Analysis	compromissioni della sicurezza derivanti da un incidente operativo o di sicurezza Minor. Il *Team* procede con una Deep Analysis *dell'incident* verificando la presenza di soluzioni a quest'ultimo: • nella Knowledge Base; • nell'elenco degli errori noti; • nei registri degli incidenti precedenti ed esistenti.	
16	**Root Cause Analysis e Lesson Learned**	A fronte di un incidente, l'incident handler raccoglie ed analizza le evidenze prodotte nella fase di gestione, al fine di identificare eventuali azioni di miglioramento. In particolare, sono agite le seguenti attività: • **raccolta, inventariazione** e corretta **conservazione** delle **evidenze** scaturite dalla gestione degli incidenti al fine di poter essere analizzate ed anche utilizzabili in caso di contenziosi; • **analisi dell'incidente** finalizzato all'individuazione delle **azioni di rimedio:** o definizione di adeguate procedure per l'analisi dei log di eventi e incidenti; o utilizzo di copie delle **evidenze** raccolte durante la fase di gestione degli incidenti per lo svolgimento delle attività di analisi a posteriori preservando in tal modo l'integrità delle evidenze originali; o contestualizzazione del processo di analisi dei dati di tracciamento in un'ottica di prevenzione volta all'individuazione di contromisure efficaci per i problemi riscontrati; o **analisi degli incidenti** più ricorrenti quantificando e monitorando tipi, volumi e impatti al fine di definire e pianificare le opportune azioni correttive anche per migliorare la capacità di prevenzione; o predisposizione di strumenti di **analisi a posteriori** basati su criteri logici che consentano l'esecuzione delle operazioni di ricerca, selezione e ordinamento dei dati raccolti; • in caso di incidenti che necessitano dell'**analisi forense**, deve essere: o predisposta un'adeguata metodologia; o prodotta copia dei supporti di memorizzazione da analizzare che garantisca la validità probatoria del supporto originale; • **Identificazioni Lesson Learned:** aggiornamento	*Incident Handler*

		delle procedure operative di risposta agli incidenti e gli scenari di test con le informazioni, i canali e le tecniche utilizzate durante la gestione dell'incidente in modo da migliorare le azioni preventive adottate e dunque prevenire il verificarsi di nuovi incidenti similari o di potenziali crisi.	
17	**Archiviazione delle informazioni**	Il processo di gestione degli incidenti si conclude tracciando le attività svolta, archiviando le evidenze prodotte e producendo la reportistica di interesse. In particolare l'incident handler: • effettua il tracciamento e l'archiviazione delle evidenze prodotte dalla gestione dell'evento; • effettua il tracciamento e l'archiviazione delle evidenze prodotte dalla gestione delle azioni di rimedio; • produce la reportistica relativa alle analisi a posteriori dell'evento; • produce la reportistica relativa alla gestione delle azioni di rimedio. Il flusso termina in tale fase.	*Incident Handler*

6 NORMATIVA DI RIFERIMENTO

6.1 NORMATIVA INTERNA

Si riepilogano le fonti informative interne alla Società che presentano relazioni con la procedura in esame:

- *Policy di Continuità Operativa del Gruppo Bancario Mediolanum (Business Continuity);*
- *Business Continuity Plan di Flowe;*
- *Policy Incident Management di Flowe;*
- *Regolamento del processo di gestione e segnalazione delle violazioni dei dati personali (data breach) di Flowe;*
- *Procedura Operativa di classificazione e segnalazione degli incidenti di Flowe.*

6.2 NORMATIVA ESTERNA

Nel presente capitolo si richiama il contesto normativo di riferimento per le attività in esame. L'elenco fornito non si ritiene esaustivo e viene riportato principalmente allo scopo di richiamare l'attenzione sui principali riferimenti, della normativa generale ed interna aziendale, sui quali si fonda la presente procedura.

- *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 2015/2366/UE (PSD2), EBA GL 2021/03 e successivi aggiornamenti;*
- *Istruzioni per la segnalazione dei gravi incidenti operativi o di sicurezza – significant institution italiane e banche autorizzate in Italia appartenenti a significant institution straniere, Banca d'Italia;*
- *Regolamento Generale sulla Protezione dei Dati - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 e successivi aggiornamenti;*
- 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;
- NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations.
- NIST Special Publication 800-61 Revision 2: Computer SecurityIncident Handling Guide.