



PROCEDURA OPERATIVA DI CLASSIFICAZIONE E SEGNALAZIONE DEGLI INCIDENTI

Procedura emessa in data 30/06/2022

Owner: *Augmented Intelligence*

SOMMARIO

1.	OBIETTIVO DEL DOCUMENTO	3
2.	AMBITO DI APPLICAZIONE	3
3.	AGGIORNAMENTO DEL DOCUMENTO	3
4.	PERIMETRO DI RIFERIMENTO	3
5.	GLI ATTORI COINVOLTI	3
5.1.	Perspective Augmented Intelligence	4
5.2.	Perspective Happiness & Services.....	5
5.3.	Business Strategy & Finance	5
5.4.	Perspective Culture Studios	5
5.5.	Utente Responsabile	5
5.6.	Funzione Risk Management	6
5.7.	Funzione Compliance.....	6
5.8.	Comitato di Crisi di Flowe	6
5.9.	Unità Organizzative della Capogruppo	7
5.9.1.	Ufficio Privacy di Banca Mediolanum	7
5.9.2.	Business Continuity Office di Banca Mediolanum	7
5.9.3.	Unità di Supporto Manageriale Service Policy & Procedures e Unità IT Security di Banca Mediolanum	8
6.	PARTNER ESTERNI	8
7.	WORKFLOW PROCEDURA OPERATIVA	9
8.	RILEVAZIONE E REGISTRAZIONE DELL'INCIDENTE	11
8.1.	Contenuti della segnalazione su DevOps.....	12
9.	CRITERI PER DETERMINARE LA TIPOLOGIA DI INCIDENTE.....	12
9.1.	Incidente operativo	12
9.2.	Incidente cyber	13
10.	ISTRUTTORIA E MODELLO DI VALUTAZIONE DI UN INCIDENTE.....	13
10.1.	Raccolta dati	18
10.2.	Classificazione dell'incidente.....	19
11.	COINVOLGIMENTO DELLA CAPOGRUPPO	19
12.	INOLTRO COMUNICAZIONE AGLI STAKEHOLDER.....	20
13.	MONITORAGGIO RISOLUZIONE INCIDENTE	20
14.	ARCHIVIAZIONE DELLE INFORMAZIONI	21
15.	RIFERIMENTI NORMATIVI	21
15.1.	Normativa esterna	22
15.2.	Normativa interna.....	22
16.	ALLEGATI.....	22

1. OBIETTIVO DEL DOCUMENTO

Obiettivo del documento è descrivere la procedura operativa di supporto alla valutazione della gravità di un incidente, così come previsto dalle “*Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica*” e degli “*Orientamenti finali in materia di segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (PSD2)*”.

Tale procedura operativa definisce l’insieme delle attività, i punti di controllo e gli strumenti utilizzati per valutare la classificazione degli incidenti di sicurezza o anche operativi, sulla base dei criteri e delle soglie definite e pubblicate da Banca d’Italia e dall’EBA.

Si precisa che a partire dal 1° gennaio 2022, avendo il Gruppo Mediolanum raggiunto soglie dimensionali rilevanti ai fini della classificazione tra le *Significant Institutions* per il passaggio alla vigilanza diretta della Banca Centrale Europea (BCE), si è prudenzialmente scelto di classificare gli incidenti secondo i criteri e le tempistiche richieste alle Banche *Significant*.

Il documento disciplina le attività in carico alle *Perspective* di Flowe e le modalità d’interazione con le altre unità organizzative coinvolte nel processo.

2. AMBITO DI APPLICAZIONE

La presente procedura si applica a Flowe S.p.A. SB. (di seguito anche “la Società”)

3. AGGIORNAMENTO DEL DOCUMENTO

L’aggiornamento del documento è a cura della *Perspective Augmented Intelligence*.

4. PERIMETRO DI RIFERIMENTO

Per “incidente operativo o di sicurezza informatica” si intende “ogni evento, o serie di eventi collegati, non pianificati dalla Società che interessa le sue risorse informatiche e che i) ha o potrebbe avere un impatto negativo sull’integrità, la disponibilità, la riservatezza e/o l’autenticità dei servizi o dei processi dell’intermediario; oppure ii) comunque implica la violazione o l’imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad esempio, frodi informatiche, attacchi attraverso *internet* e malfunzionamenti e disservizi).

Un evento relativo alla sicurezza delle informazioni corrisponde al verificarsi di un determinato stato del sistema, del servizio o della rete indicante una possibile violazione della policy di sicurezza delle informazioni o un’inefficienza dei presidi, o al prodursi di una situazione ignota che può comportare conseguenze per la sicurezza (**ISO IEC 27001:2005(E)**).

Si specifica infine che il perimetro definito implica anche il coinvolgimento di partner esterni; i più rilevanti, per volumi di transazioni gestite, sono Temenos e Nexi¹.

5. GLI ATTORI COINVOLTI

Gli attori, ovvero le unità organizzative aziendali coinvolte a vario titolo nel processo di classificazione e segnalazione dei gravi incidenti sono di seguito elencati, con evidenza esclusivamente del ruolo specificatamente attribuito nel processo medesimo.

¹ SIA sino alla fusione per incorporazione di questa in NEXI avvenuta il 16 dicembre 2021.

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. Nell'attività/servizio interessato dall'evento (*service level agreement* - SLA e *key performance indicator* - KPI), al fine di garantirne il corretto funzionamento;

5.1. **Perspective Augmented Intelligence**

La *Perspective Augmented Intelligence* e specificatamente il *Team IT Operation, Security & Governance*, nell'ambito della presente procedura operativa:

- riceve tutte le segnalazioni relative agli incidenti operativi e di sicurezza “rilevanti” e avvia, con il supporto delle unità organizzative coinvolte e delle strutture di controllo, la raccolta dei dati necessari alla relativa valutazione di impatto²;
- segnala, secondo opportuni criteri di proporzionalità, all'Unità di Supporto Manageriale *Service Policy & Procedures*, all'interno della *Direzione Service, Operations & ICT* di Banca Mediolanum gli incidenti in tema PSD2 e all'Unità *IT Security* di Banca Mediolanum gli incidenti cyber;
- ai fini della classificazione dell'incidente, effettua le analisi, applicando i parametri e le soglie previste dalle istruzioni per la segnalazione dei gravi incidenti ai sensi delle Istruzioni per la segnalazione dei gravi incidenti operativi o di sicurezza - *significant institution* italiane;
- qualora si profilasse un evento che si avvicini al raggiungimento delle soglie di un criterio di High Impact Level o più criteri di Lower Impact, il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* provvede a convocare il Comitato di Crisi di Flowe;
- predispone per il Comitato di Crisi di Flowe, un documento con i dati utilizzati per formulare la proposta di classificazione dell'incidente e fornisce allo stesso Comitato il totale delle transazioni interessate ed il numero dei pagamenti compromessi, come percentuale del livello normale delle transazioni di pagamento effettuate mediante i servizi interessati ed il numero di utenti del servizio, ovvero tutti i clienti che hanno un contratto per l'accesso al servizio di interessato colpito dall'incidente, sia in termini assoluti sia in percentuale rispetto al numero totale di utenti del servizio, al fine di consentire una valutazione rispetto ai criteri di classificazione determinati dalla normativa di riferimento e riportati più avanti al paragrafo 10.
- in collaborazione con le Funzioni Aziendali di Controllo, e gli altri attori necessari in base al tipo di incidente rilevato (es.: *Business Continuity Office, Risk Management*) supporta *Service, Policy & Procedures* ed *IT Security* di Banca Mediolanum - in base al tipo di incidente - per la predisposizione dei Report e invio all'Autorità di Vigilanza;
- presidia 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 al Comitato di Crisi di Flowe;
- tiene traccia di tutti gli incidenti 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;

² Per gli incidenti operativi senza impatto sui servizi di pagamento, è l'Utente Responsabile dell'applicazione impattata la figura di riferimento per la raccolta delle informazioni sull'incidente che fornisce supporto al *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence*.

- verifica la fondatezza delle segnalazioni di eventuali *Data Breach* rilevati dalle *Perspective* e li segnala all'Ufficio Privacy di Banca Mediolanum;
- è responsabile della predisposizione e manutenzione della reportistica utile a rilevare il numero di Clienti e transazioni potenzialmente coinvolti dall'incidente operativo o di sicurezza;

5.2. **Perspective Happiness & Services**

La *Perspective Happiness & Services*, è responsabile, in linea con le relative policy, della gestione e del controllo dei flussi di acquisizione delle disposizioni della clientela su prodotti/servizi bancari, dell'espletamento dei controlli formali e dello svolgimento dei processi operativi di competenza, nel rispetto dei livelli di servizio e degli standard di qualità definiti. La *Perspective* ha inoltre la responsabilità delle richieste di chiarimento, di verifica o di rettifica pervenute dalla clientela.

Nell'ambito della presente procedura operativa, la stessa, in coerenza con la propria mission:

- segnala tempestivamente al *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* gli incidenti in generale ed in particolare quelli operativi o di sicurezza desumibili a partire da reclami ricevuti dalla clientela o comunque rilevati nello svolgimento delle attività di competenza della *Perspective*;
- fornisce supporto al *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* nel corso dell'intero processo di gestione dell'incidente, coinvolgendo gli outsourcer per raccogliere dati utili alla classificazione dello stesso, predisporre i report per l'Autorità di Vigilanza, contribuire alla gestione dei follow-up;
- partecipa al processo di definizione dei contenuti e dei canali delle eventuali comunicazioni nei confronti dei clienti.

Nel caso di incidenti classificati come "gravi", in collaborazione con la *Perspective Culture Studios* predispone i contenuti della comunicazione da inviare alla clientela con il supporto della Consulenza Legale di Banca Mediolanum in qualità di outsourcer.

5.3. **Business Strategy & Finance**

L'unità *Business Strategy & Finance* supporta il processo di valutazione dell'incidente, al fine di individuare eventuali *major incident*.

5.4. **Perspective Culture Studios**

La *Perspective Culture Studios*, nell'ambito della presente procedura, cura la gestione delle eventuali iniziative di comunicazione alla clientela di Flowe, definendone gli standard e il contenuto.

5.5. **Utente Responsabile**

L'Utente Responsabile è la figura di riferimento aziendale, identificata per ciascun sistema o applicazione, ovvero assume il ruolo di referente interno dell'applicazione e ne assume formalmente la responsabilità, in rappresentanza degli utenti e nei rapporti con le funzioni preposte allo sviluppo e alla gestione tecnica.

Per le applicazioni afferenti a diverse *Perspective*, l'Utente Responsabile è identificato sulla base del principio di prevalenza, ovvero in base al processo da cui l'applicazione maggiormente dipende.

Nell'ambito della presente procedura operativa, l'Utente Responsabile è il referente delle attività di raccolta delle informazioni dei gravi incidenti operativi o di tipo *cyber* che non hanno impatto sui servizi di pagamento. In particolare, collabora con il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* per la raccolta dei dati necessari alla valutazione della «gravità» dell'incidente (es.: impatto reputazionale, economico, durata del disservizio) e per la classificazione dell'incidente («potenzialmente grave» vs «non grave»).

5.6. Funzione Risk Management

La funzione '*Risk Management*' verifica, raccoglie e riconcilia, con il supporto delle altre unità organizzative, 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 delle segnalazioni all'Autorità di Vigilanza. Sono inclusi, i gravi incidenti operativi non legati ai servizi di pagamento, da segnalare alla Capogruppo.

Coordinandosi con *Business Strategy & Finance* e la *Perspective Happiness & Service* effettua una valutazione circa l'impatto reputazionale derivante dall'incidente rilevato.

5.7. Funzione Compliance

La *Funzione Compliance*, comunque inserita nel Comitato di Crisi di Flowe, collabora - ove richiesto - al processo di segnalazione dei *major incident* fornendo alle *Perspective* preposte di Flowe informazioni a supporto della valutazione di eventuali violazioni di obblighi regolamentari derivanti dal *major incident*.

5.8. Comitato di Crisi di Flowe

Il Comitato di Crisi di Flowe è composto dall'Amministratore Delegato, dai responsabili di *Perspective*, dai responsabili delle strutture di controllo, dal Responsabile ICT e dal responsabile della *Business Continuity*, a titolo consultivo coinvolge anche le funzioni di controllo della capogruppo:

- Service Policy & Procedures;
- Organizzazione e Project Management;
- IT User Support & Service Management.

Il Comitato di Crisi di Flowe esamina le evidenze dell'istruttoria condotta dal *Team IT Operation, Security & Governance* della *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.

Nelle fasi successive alla prima segnalazione, il Comitato 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.

Inoltre, il Comitato di Crisi di Flowe può convocare il Comitato di Gestione della Crisi della Capogruppo in caso di grave incidente senza impatto sulla Capogruppo stessa che, in questo caso non è responsabile della delibera della gravità dell'incidente, ma esamina le valutazioni effettuate dalla Società e discute i possibili impatti dell'evento sulla Capogruppo; nella predetta casistica, partecipano alla seduta del Comitato

l'Amministratore Delegato, il Direttore Generale e il Responsabile delle Funzioni *Risk Management* e Compliance della Società impattata dall'incidente.

5.9. Unità Organizzative della Capogruppo

Le unità organizzative della Capogruppo coinvolte nel processo sono:

5.9.1. Ufficio Privacy di Banca Mediolanum

L'Ufficio Privacy di Banca Mediolanum, ingaggiato dal *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* che laddove questa 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 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 incidenti definito su *Azure DevOps*.

5.9.2. Business Continuity Office di Banca Mediolanum

Il *Business Continuity Office* (di seguito anche *BC Office*), 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.

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* della *Perspective Augmented Intelligence*, 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 il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* nella predisposizione della documentazione utile al Comitato di Crisi di Flowe;
- collabora alla compilazione delle sezioni del report intermedio di segnalazione relative alle tempistiche e modalità di attivazione del piano di continuità operativa e/o del piano di *Disaster Recovery* (solo nel caso di attivazione dei predetti piani).

5.9.3. Unità di Supporto Manageriale Service Policy & Procedures e Unità IT Security di Banca Mediolanum

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 *cyber*) nell'ambito della presente procedura operativa:

- riceve dal *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* le segnalazioni relative agli incidenti operativi e di sicurezza "rilevanti";
- 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.

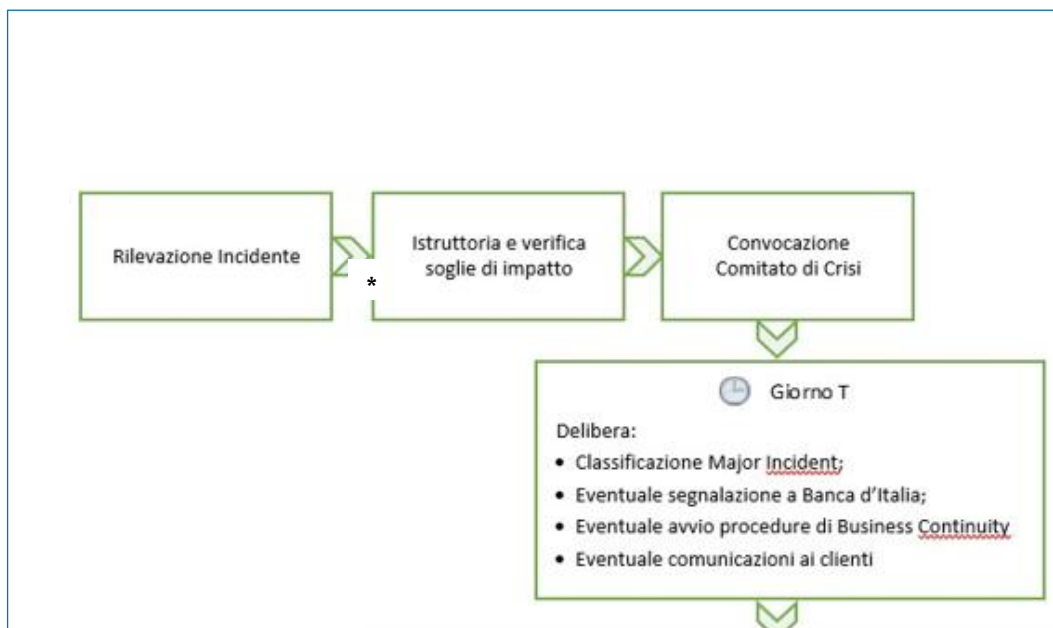
6. PARTNER ESTERNI

Nell'ambito della presente procedura operativa si definisce **partner esterno**, un qualunque fornitore con il quale è in essere un contratto di *Outsourcing, Application Management, Servicing* relativo ai servizi di pagamento elettronico.

A seguito della rilevazione di un incidente operativo o di sicurezza in ambito alla presente procedura, il partner esterno:

- segnala l'evento alla *Perspective* di riferimento.
- è responsabile delle attività di analisi e diagnosi dell'incidente e della relativa risoluzione, della raccolta dei dati necessari all'istruttoria e dell'inoltro alla *Perspective* di riferimento, che a sua volta provvede ad attivare il processo di classificazione della gravità dell'incidente.
- monitora l'incidente e fornisce alla Società continui aggiornamenti in merito allo stato di risoluzione e fornisce le informazioni necessarie alla predisposizione dei rapporti.
- fornisce alla Società anche ulteriori informazioni relative all'incidente grave a supporto delle attività post chiusura.

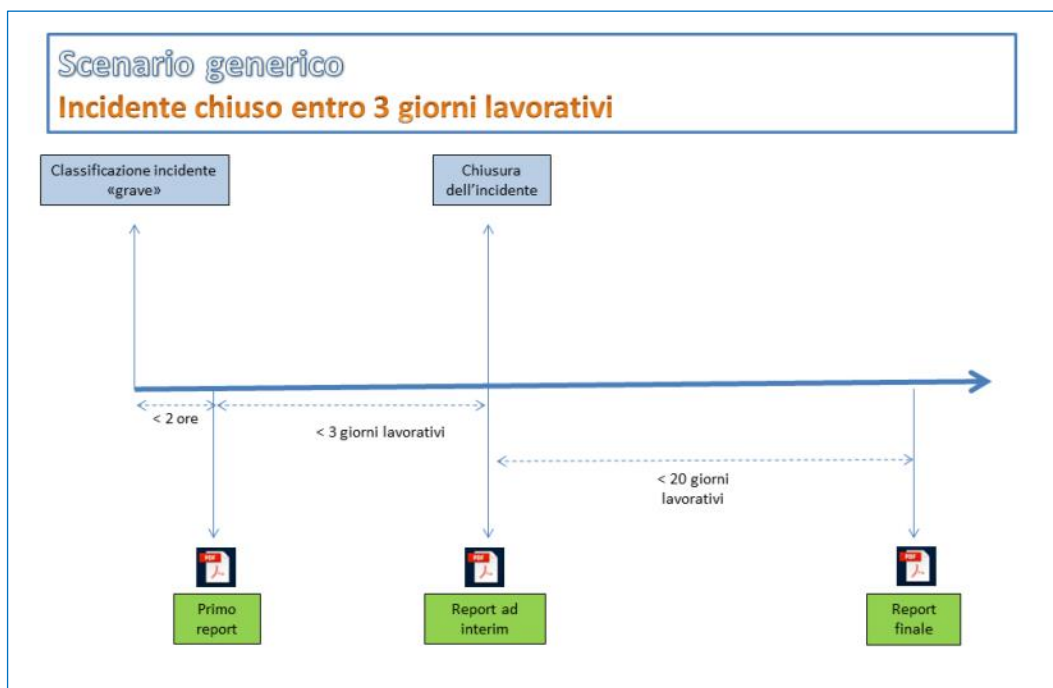
7. WORKFLOW PROCEDURA OPERATIVA



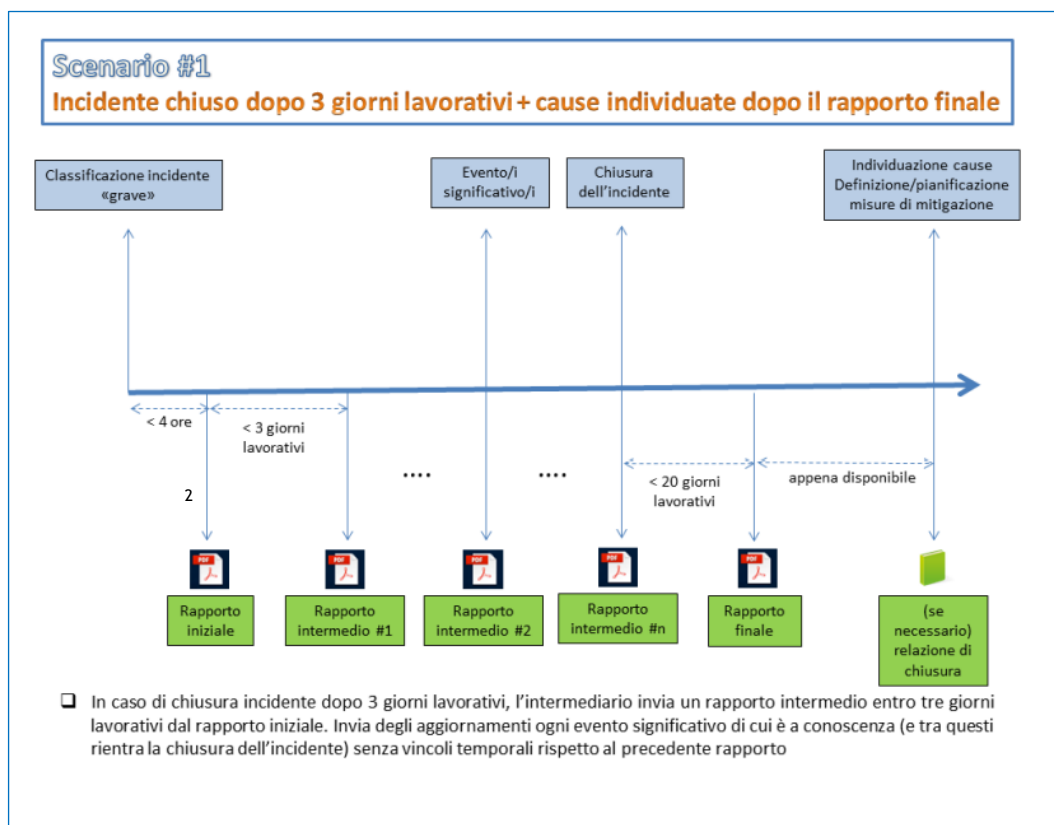
*ed eventuale registrazione su DevOps

Si riportano di seguito i possibili scenari di segnalazione a Banca d'Italia conformemente alle Istruzioni per la segnalazione dei gravi incidenti operativi o di sicurezza - per le banche *significant*:

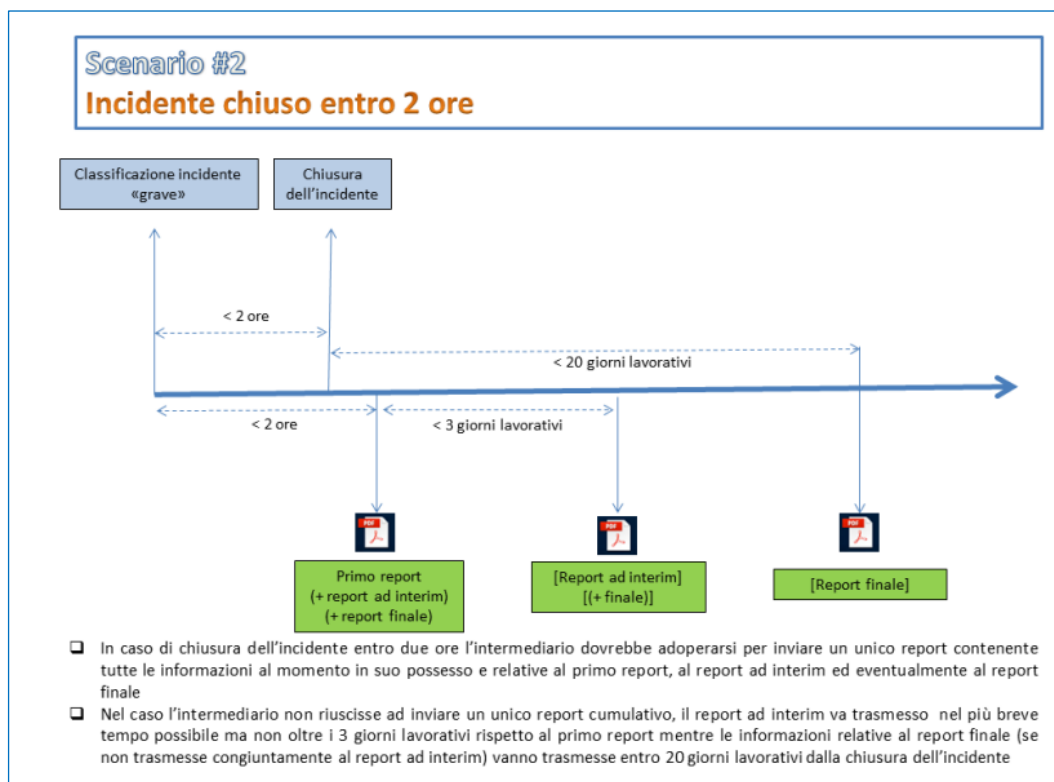
Scenario 1:



Scenario 2:



Scenario 3:



Si specifica che le attività disciplinate nel corso dei prossimi paragrafi della procedura sono svolte, coerentemente con le tempistiche previste dalle istruzioni operative di Banca d'Italia, durante l'orario lavorativo (lun - Ven ore 9.00-18.00) delle giornate operative di Flowe⁴.

8. RILEVAZIONE E REGISTRAZIONE DELL'INCIDENTE

Gli incidenti causati da errori operativi o di sicurezza informatica possono essere rilevati da attori interni o esterni alla Società. Di seguito si riportano degli esempi sui potenziali attori coinvolti e relative modalità di rilevazione:

- *Perspective Happiness & Services*, a seguito di:
 - segnalazioni (singole o massive) avanzate dai Clienti;
 - approfondimenti di casistiche rilevate o segnalate dalle unità organizzative di *front office* o di *back office*;
 - segnalazioni derivanti da reclami dei Clienti che possano segnalare un incidente;
 - segnalazioni di disconoscimento di operazioni;
 - Indicazioni degli *outsourcer*, che segnalano gli incidenti coerentemente con le policy operative definite da Flowe per il proprio sistema informativo.
- *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence*, a seguito dell'attività di monitoraggio continuo dei sistemi e del database degli incident su *Azure DevOps*.

A fronte di ogni anomalia rilevata sui sistemi informativi, gli operatori di Flowe effettuano una valutazione preliminare al fine di stabilire se la stessa debba essere registrata nell'apposito database degli *incident* su *Azure DevOps*. Dovrebbero essere registrati tutti gli *incident* che l'operatore ritiene essere rilevanti e comunque tutti quelli che realizzano almeno una delle seguenti condizioni:

- Durata superiore alle 2 ore;
- Impatto sulla clientela diretto o indiretto a livello sistemico;
- Replica dell'incidente in almeno 3 occasioni nei 10 giorni precedenti.

Tutte le altre tipologie di eventi non derivanti da malfunzionamenti o da errori di sicurezza dei sistemi informativi rilevati dai *team* delle *Perspective* interessate e dai relativi *outsourcer* sono invece inoltrati tramite e-mail al Responsabile della *Perspective* stessa.

Analogamente, nei casi in cui l'incidente applicativo o il fermo del servizio sia rilevato da partner esterni, il partner esterno stesso invia la comunicazione alla *Perspective di riferimento* che in caso di incidente grave estende l'informativa al *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence*.

Qualora un incidente non sia chiaramente riconoscibile come un'anomalia o un errore, ma sussista il dubbio che possa esserlo, la *Perspective* che lo rileva, informa il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* per una valutazione preliminare.

La *Perspective* che registra l'*incident* sul db invia sempre un messaggio di allarme al *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence*. L'ownership dell'*incident* è in carico all'operatore che ne ha effettuato il censimento a meno che il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* ritenga che ricorrano gli estremi per evocarne a se la gestione e richieda alla *Perspective* che ha rilevato

⁴ In particolare, Flowe ha stabilito un cut-off (h 18.00) per regolare in Rete Interbancaria le operazioni di pagamento elettronico disposte dalla clientela. Le disposizioni ricevute oltre tale orario vengono regolate il giorno lavorativo successivo.

l'incident il trasferimento dell'*ownership* al *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* .

8.1. Contenuti della segnalazione su DevOps

La segnalazione dell'incidente, censita su *DevOps* dalla *Perspective* che lo rileva, contiene le seguenti informazioni:

- la classificazione dell'incidente, selezionando una delle opzioni disponibili;
- l'impatto che l'*incident* ha determinato o potrebbe determinare, selezionando una delle opzioni disponibili;
- 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.

9. CRITERI PER DETERMINARE LA TIPOLOGIA DI INCIDENTE

Come disposto dalle Istruzioni per la segnalazione dei gravi incidenti operativi o di sicurezza - delle banche *significant* tutti i possibili incidenti oggetto della presente procedura operativa appartengono ad una (ed una sola) delle due tipologie:

9.1. Incidente operativo

Incidenti 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*.

Rientrano in questa tipologia le seguenti categorie di incidenti:

- eventi accidentali (e.g. errore umano con eccezione della diffusione/alterazione di dati accidentale, classificata in questo contesto come *cyber*);
- malfunzionamento del processo come conseguenza dell'inadeguata progettazione o esecuzione del processo, dei controlli di processo e/o dei processi di supporto (ad esempio, processo per modifica/migrazione, test, configurazione, capacità, monitoraggio);
- problema software in conseguenza del malfunzionamento di programmi software applicativi o di base;
- problema hardware o infrastrutturale dovuti a malfunzionamenti di sistemi e componenti hardware ovvero di reti di comunicazione o piattaforme condivise;
- sabotaggio di apparati tramite accesso fisico;

- evento naturale dovuto a cause naturali o esterne, come inondazioni, incendi, terremoti.

9.2. Incidente cyber

Incidenti causati da attività volontaria e malevola riguardanti l'accesso, l'uso, la divulgazione, l'interruzione, la modifica o la distruzione non autorizzati delle risorse della Società o incidenti che comunque producono, anche involontariamente, diffusione e/o alterazione di dati riservati della clientela e/o dell'intermediario.

Rientrano in questa tipologia le seguenti categorie di incidenti:

- esecuzione di software (malware) su sistemi di elaborazione fissi o mobili al fine di ostacolarne le operazioni, sottrarre informazioni sensibili, accedere a sistemi informatici privati o mostrare pubblicità indesiderata;
- social engineering (ingegneria sociale): manipolazione psicologica degli individui volta ad indurre determinate azioni o a divulgare informazioni riservate;
- pretexting (creazione di un pretesto) creazione e utilizzo di uno scenario inventato (il pretesto) per coinvolgere un determinato utente in modo tale da aumentare le possibilità che divulghi informazioni o agisca secondo modalità improbabili in circostanze normali;
- phishing ovvero il tentativo di carpire informazioni sensibili come nomi utente, password e dati di carte di credito (nonché talvolta, indirettamente, denaro), spesso a scopo fraudolento, operato fingendo di essere un soggetto affidabile in una comunicazione elettronica. I tentativi di phishing sono generalmente rivolti a persone con accesso privilegiato a informazioni o sistemi transazionali. Per aumentare le probabilità di successo, è possibile che gli aggressori acquisiscano informazioni personali sul loro target;
- minaccia posta in essere dal personale interno o da un fornitore terzo (insider/third party provider threat) derivante dalla violazione delle policy di sicurezza o dei diritti di accesso;
- accesso non autorizzato (unauthorised access) posto in essere da un soggetto (hacker) che accede illecitamente a reti, dati o sistemi attraverso il tentativo di utilizzo di tutte le possibili chiavi di accesso al sistema (brute-force attack) oppure il tentativo di indovinare la chiave, solitamente creata dalla password attraverso una funzione di derivazione;
- negazione di servizi (denial of service, DoS) ovvero un malfunzionamento dovuto ad un attacco informatico in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio, si verifica spesso nella veste di attacco distribuito (distributed denial of service, DDoS) in cui il traffico dei dati in entrata che inonda la vittima proviene da molte fonti diverse per impedire la difesa attraverso il blocco di una singola fonte;
- minaccia persistente avanzata (advanced persistent threat) ovvero un insieme di processi occulti e continui di intrusione informatica per il monitoraggio o l'estrazione di dati da un obiettivo specifico. Questo tipo di attacco consiste solitamente in una pluralità di altre tipologie attuate per un lungo periodo di tempo.

10. ISTRUTTORIA E MODELLO DI VALUTAZIONE DI UN INCIDENTE

Una volta ricevuta la segnalazione, il responsabile del *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence*, o il suo delegato, raccoglie tutti i dati e traccia le attività di istruttoria per classificare eventualmente l'incidente come "major".

I parametri sulla base dei quali valutare la "gravità" di un incidente sono i seguenti:

Al verificarsi di un incidente operativo o di sicurezza, il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* valuta la rilevanza utilizzando i criteri di seguito specificati e lo classifica conseguentemente come “grave” o “non grave” ai fini della segnalazione.

È da considerarsi come incidente ‘grave’ quando è soddisfatto anche uno solo dei criteri:

- a) *Incident publicly reported and/or can cause significant reputational damage* (Un incidente operativo o di sicurezza è reso pubblico e/o può comportare **importanti danni reputazionali**). È da considerarsi “grave” un incidente che riceva (o che probabilmente riceverà) attenzione mediatica a livello locale, nazionale o internazionale da parte dei quotidiani o delle agenzie di stampa la cui diffusione è importante per la Società. Qualora riguardi un’area operativa critica per la fiducia dei clienti (a prescindere dal fatto che i sistemi coinvolti siano gestiti all’interno dell’azienda o attraverso fornitori o terze parti) e abbia una portata significativa, l’incidente deve essere classificato come rilevante ai fini della segnalazione anche se non ha ricevuto un’attenzione mediatica considerevole. Ad esempio, quando:

- si verifichi una fuga/sottrazione di dati dai conti dei clienti;
- siano stati compromessi i sistemi di pagamento;
- vengano pregiudicati/sottratti dati personali.

Inoltre, nel caso l’incidente abbia impatto sui servizi di pagamento gli intermediari considerano se (i) gli utenti di servizi di pagamento e/o altri prestatori di servizi di pagamento si sono lamentati dell’impatto negativo dell’incidente, (ii) l’incidente ha influito su un processo visibile e pertanto riceverà probabilmente o ha già ricevuto copertura mediatica (non solo tramite i media tradizionali, come i giornali, ma anche blog, social networks, ecc.), (iii) sono stati o saranno probabilmente disattesi obblighi contrattuali, con la conseguente pubblicazione di azioni legali contro il prestatore di servizi di pagamento (iv) non si sono adempiuti obblighi regolamentari con la conseguente imposizione di misure di vigilanza o sanzioni che sono state o saranno probabilmente rese pubbliche o, (v) lo stesso tipo di incidente si è già verificato in passato.

- b) *Estimated financial impact is above EUR 5M or max (0.1% of CET1 capital; 200.000 EUR)* (L’**impatto finanziario** stimato dell’incidente operativo o di sicurezza supera i cinque milioni di euro o il massimo tra lo 0,1 per cento del capitale primario di classe 1 (Common Equity Tier 1) dell’intermediario e 200.000 EURO.)

L’impatto finanziario va valutato in un’ottica globale. Nel caso non risulti possibile una valutazione dettagliata e precisa dell’impatto finanziario, si dovrà ricorrere a stime. L’impatto finanziario dovrà comunque considerare qualsiasi costo collegato direttamente o indirettamente all’incidente come:

- fondi o beni sottratti;
- costi per la sostituzione di hardware e software;
- altri costi di indagine e di ripristino dei danni (ad esempio revisori esterni, negoziazione di nuovi contratti, ricerca di nuovi fornitori);
- sanzioni per l’inosservanza di obblighi contrattuali;
- mancati introiti dovuti ad interruzioni di servizi;
- mancati ricavi dovuti alla perdita di opportunità commerciali;
- potenziali spese legali.

- c) *High internal escalation (Alto livello di escalation interna)*

La dimensione dell’incidente è tale che il Comitato di Crisi di Flowe convocato dal *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence*

ne conferma la natura di *major incident* anche in mancanza del raggiungimento delle altre soglie qualitative/quantitative.

- d) *Incident is likely to lead to breaches of legal or regulatory obligations* (L'incidente operativo o di sicurezza comporta verosimilmente la **violazione di obblighi legali o regolamentari**.)

Esempi di violazione di obblighi legali o regolamentari includono:

- il mancato rispetto di scadenze per segnalazioni regolamentari o fiscali;
- l'incapacità di adempiere a obblighi riguardanti i clienti (ad esempio esecuzione di transazioni, pagamento di garanzie, trasferimenti di denaro);
- la violazione di sanzioni o normative inerenti al riciclaggio o al finanziamento del terrorismo (ad esempio per inadempimento degli obblighi di adeguata verifica).

Anche un incidente che ha alte probabilità di coinvolgere la Società in un numero elevato di azioni legali va classificato come "grave".

- e) *Crisis management procedures triggered or is likely to be called upon* (L'incidente operativo o di sicurezza innesca o potrebbe innescare procedure di gestione della **continuità operativa** o di gestione delle crisi.)

Include i seguenti casi:

- A. L'incidente operativo o di sicurezza provoca o potrebbe provocare l'attivazione del piano di continuità operativa (business continuity plan, BCP) ovvero l'attivazione:
- del piano di disaster recovery (disaster recovery plan, DRP);
 - delle comunicazioni di emergenza e allerta dei membri dei team addetti al disaster recovery e di altri soggetti coinvolti;
 - delle procedure di backup e ripristino (in formato cartaceo ed elettronico) dei dati;
 - del riavvio di tutti i sistemi a elevata criticità dopo un incidente al fine di assicurare il tempestivo ripristino della normale operatività, avuto specifico riguardo ai tempi ed ai punti di ripristino fissati per i processi critici e di rilevanza sistemica;
 - delle valutazioni finanziarie e operative al fine di identificare cambiamenti nell'esposizione al rischio operativo, finanziario e creditizio a seguito di un incidente;
 - dei processi di segnalazione regolamentare avviati dopo un incidente allo scopo di garantire il costante rispetto degli obblighi di segnalazione regolamentare;
 - dei processi per fornire ai clienti immediato accesso ai loro fondi e titoli dopo che un incidente ha provocato l'interruzione dei sistemi utilizzati per la gestione di fondi e titoli.
- B. Si fa valere la polizza contro i rischi informatici (*cyber insurance*) per coprire le perdite finanziarie derivanti dall'incidente.
- C. L'incidente operativo o di sicurezza attiva o potrebbe attivare altre procedure di gestione delle crisi.
- f) *Transactions affected* - High impact (**Transazioni interessate** - Alto impatto)
- Nel caso di incidente che coinvolge servizi di pagamento della Società, il numero di transazioni interessate è maggiore del 25% del livello normale delle transazioni della Società (in termini di numero di transazioni) o di 15 milioni di EUR.

La Società determina il valore totale delle transazioni interessate e il numero dei pagamenti compromessi come percentuale del livello normale delle transazioni di pagamento effettuate mediante i servizi di pagamento interessati.

Come regola generale, la Società deve considerare come «transazioni interessate» tutte le transazioni nazionali e transfrontaliere che sono state o probabilmente saranno interessate, direttamente o indirettamente, dall'incidente e, in particolare, quelle transazioni che potrebbero non essere iniziate o elaborate, quelle per le quali il contenuto del messaggio di pagamento è stato alterato e quelle ordinate in modo fraudolento (a prescindere dal fatto che i fondi siano stati recuperati o meno).

Inoltre, la Società deve intendere come livello normale di transazioni di pagamento la media annuale giornaliera delle transazioni di pagamento nazionali e transfrontaliere effettuate con gli stessi servizi di pagamento interessati dall'incidente, prendendo l'anno precedente come periodo di riferimento per i calcoli.

g) *Users affected* - High impact (**Utenti interessati** - Alto impatto)

Il numero di utenti del servizio offerto dalla Società interessati dall'incidente è maggiore di 50 000 o del 25% del numero totale di utenti del servizio.

La Società determina il numero di utenti del servizio interessati, sia in termini assoluti sia in percentuale del numero totale di utenti del servizio interessato dall'incidente.

La Società considera come «utenti del servizio» tutti i clienti (nazionali o stranieri, consumatori o imprese) che hanno un contratto con la Società che garantisce loro l'accesso al servizio interessato e che hanno subito o probabilmente subiranno le conseguenze dell'incidente. La Società deve ricorrere a stime basate sull'attività precedente per determinare il numero di utenti del servizio interessato dall'incidente che potrebbero aver utilizzato il servizio nel corso dell'incidente.

Nel caso la Società offrisse servizi operativi a terzi, deve considerare solo i propri utenti (se ve ne sono) e gli intermediari che ricevono tali servizi operativi devono valutare l'incidente in relazione ai propri utenti.

Inoltre, la Società considera quale numero totale di utenti il numero aggregato degli utenti nazionali e transfrontalieri contrattualmente vincolati al momento dell'incidente (o, in alternativa, il numero più recente disponibile) e aventi accesso al servizio interessato, a prescindere dalla loro dimensione o dal fatto che siano ritenuti utenti attivi o passivi.

h) quando **tre** delle seguenti quattro condizioni, valutate singolarmente come **impatti "minori"**, si rilevino nell'ambito dei servizi di pagamento contemporaneamente:

h.a) *Transactions affected* - Low impact (Transazioni interessate - Basso impatto)

Il numero di transazioni interessate è maggiore del 10% del livello normale delle transazioni della Società (in termini di numero di transazioni) o di EUR 500.000.

Nel caso di incidenti operativi che influiscono sulla capacità della Società di avviare e/o elaborare transazioni il criterio è soddisfatto solo se la durata dell'incidente è superiore ad un'ora.

h.b) *Users affected* - Low impact (Clienti interessati - Basso impatto)

Il numero di utenti del servizio offerto dalla Società interessati dall'incidente è maggiore di 5.000 o del 10% del totale del numero di utenti del servizio.

Nel caso di incidenti operativi che influiscono sulla capacità dell'intermediario di avviare e/o elaborare transazioni il criterio è soddisfatto solo se la durata dell'incidente è superiore ad un'ora.

h.c) *Service downtime* (Indisponibilità del servizio)

Il periodo di indisponibilità del servizio di pagamento è maggiore di 2 ore.

La Società determina il periodo di tempo in cui il servizio probabilmente non sarà disponibile all'utente del servizio di pagamento o in cui l'ordine di pagamento, inteso ai sensi dell'articolo 4, paragrafo 13, della PSD2, non potrà essere eseguito. La Società considera il periodo di tempo in cui qualsiasi attività, processo o canale che abbia un collegamento con la prestazione di servizi di pagamento è o sarà probabilmente interrotto, impedendo di conseguenza (i) l'avvio e/o l'esecuzione di un servizio di pagamento e/o (ii) l'accesso a un conto di pagamento. Il periodo di indisponibilità del servizio è calcolato dal momento del suo inizio e devono essere considerati sia gli intervalli di tempo in cui sono operativi, come richiesto per l'esecuzione dei servizi di pagamento, sia gli orari di chiusura e i periodi di manutenzione, se del caso e se applicabile. Se l'intermediario non è in grado di determinare il momento di inizio del periodo di inattività del servizio, deve eccezionalmente calcolare tale periodo a partire dal momento in cui l'indisponibilità è stata rilevata.

h.d) *Breach of security of network or information systems* (Violazione della sicurezza della rete o dei sistemi informativi)

La Società determina se un'azione dolosa ha compromesso la disponibilità, l'autenticità, l'integrità o la riservatezza della rete o dei sistemi informativi (inclusi i dati) relativi alla prestazione di servizi di pagamento.

i) *Incident may affect other institutions/organisations (systemic impact)* (L'incidente può interessare altre istituzioni/organizzazioni (**impatto sistemico**))

L'incidente deve essere classificato come grave nell'ambito del presente framework se si ritiene che l'incidente abbia alte probabilità di:

- essere replicato presso altri istituti (ad esempio perché ha evidenziato carenze condivise in materia di sicurezza);
- incidere sulla solidità dell'intero sistema finanziario. Ciò potrebbe verificarsi quando:
 - un altro intermediario è stato recentemente oggetto di un attacco simile (per esempio la notizia è apparsa sulla stampa);
 - l'incidente evidenzia gravi vulnerabilità che possono essere comuni ad altri istituti.

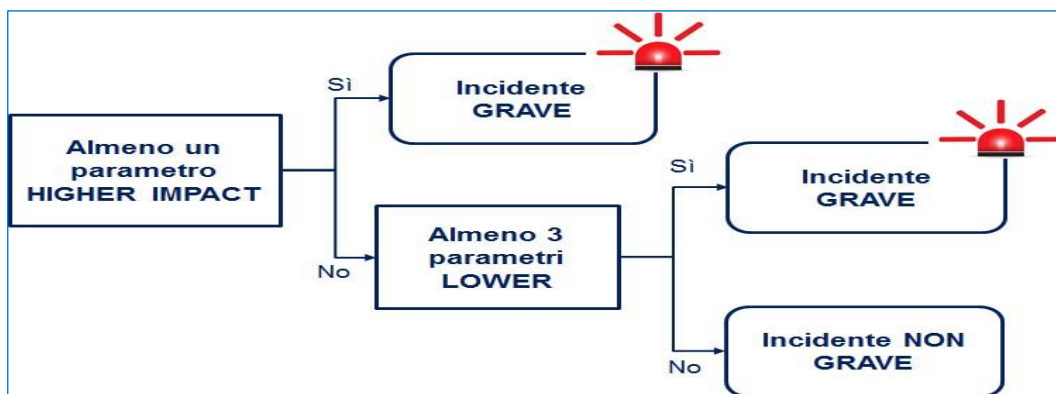
La Società, inoltre valuta l'impatto dell'incidente sui mercati finanziari, intesi come le infrastrutture dei mercati finanziari e/o gli schemi di pagamento che li supportano e altri prestatori di servizi di pagamento.

j) *Incident is reported to the national CERT/CSIRT, security agency or police (only cyber)* (L'**incidente è comunicato al CERT** (Computer Emergency Response Team) nazionale o al Computer Security Incident Response Team (CSIRT), ad un'agenzia di sicurezza governativa o alla polizia (solo incidenti cyber))

Il presente criterio si applica solo in caso di incidenti *cyber*.

L'incidente deve essere classificato come grave se comunicato a:

- CERT/CSIRT nazionale;
- Un'agenzia di sicurezza governativa che conduce attività di intelligence per la sicurezza nazionale o è responsabile del coordinamento delle attività di sicurezza *cyber*;
- Polizia nazionale o internazionale (e.g. Europol).



L'attribuzione della tipologia e della classe degli *Incident* significativi è condivisa con l'Unità di Supporto Manageriale Service Policy & Procedures, all'interno della Direzione Service, Operations & ICT di Banca Mediolanum (per incidenti in tema PSD2), con l'Unità IT Security di Banca Mediolanum (per incidenti in tema cyber), con l'Ufficio Privacy di Banca Mediolanum (in caso di *data breach*) oppure con l'Utente Responsabile (in caso di incidenti operativi senza impatto sui servizi di pagamento).

Altre valutazioni: qualora sulla base dei precedenti criteri l'incidente non risultasse di grave entità, il Comitato di Crisi di Flowe in collaborazione con l'Unità di Supporto Manageriale Service Policy & Procedures, all'interno della Direzione Service, Operations & ICT di Banca Mediolanum (per incidenti in tema PSD2), l'Unità IT Security di Banca Mediolanum (per incidenti in tema cyber), con l'Ufficio Privacy di Banca Mediolanum (in caso di *data breach*) o con l'Utente Responsabile (in caso di incidenti operativi senza impatto sui servizi di pagamento) ha comunque la possibilità di considerarlo tale; più precisamente, può comunque segnalare l'incidente all'Autorità di Vigilanza nel caso in cui individui un'importante interruzione dei servizi, un danno reputazionale, un impatto legale o regolamentare, uno svantaggio competitivo o un potenziale impatto sistemico. Se la valutazione della rilevanza non conduce a un risultato chiaro (ad esempio non è chiaramente distinguibile il perimetro dell'incidente, le entità coinvolte e le corrispondenti soglie relative ai criteri di rilevanza), l'incidente è da considerarsi grave. Qualora diversi incidenti appaiano tra loro collegati, Flowe deve avvalersi delle valutazioni dei propri esperti per decidere se tali eventi determinino un unico incidente o corrispondano a più incidenti.

L'Unità di Supporto Manageriale Service Policy & Procedures, (per incidenti in tema PSD2), l'Unità IT Security di Banca Mediolanum (per incidenti in tema cyber), l'Ufficio Privacy di Banca Mediolanum (in caso di *data breach*) e l'Utente Responsabile (in caso di incidenti operativi senza impatto sui servizi di pagamento) sono coinvolte anche qualora il Team IT Operation, Security & Governance della Perspective Augmented Intelligence rilevi dubbi sulla misura dei parametri considerati.

10.1. Raccolta dati

Il Team IT Operation, Security & Governance della Perspective Augmented Intelligence, non appena a conoscenza dell'incidente, avvia il processo di raccolta dati al fine dell'eventuale segnalazione alle Autorità di Vigilanza avvalendosi del supporto delle altre perspective.

In caso di fermo totale dei servizi a seguito di un incidente, appena possibile dalla rilevazione del disservizio, la Perspective Happiness & Services (in base al tipo di incidente) aggiorna il Team IT Operation, Security & Governance della Perspective Augmented Intelligence in merito alle indagini in corso sull'evento che potrebbe aver

causato l'incidente e sull'ipotesi dei tempi di ripristino dei servizi. Tale aggiornamento avviene in modo frequente e costante.

In caso di fermo parziale dei servizi a seguito di un incidente che impatta i servizi di pagamento e permette comunque di processare alcune transazioni di pagamento, la *Perspective Happiness & Services* (in base al tipo di incidente), oltre agli aggiornamenti sopra indicati fornisce, sempre in modo frequente e costante, anche un report delle operazioni di pagamento andate a buon fine, tipo di disposizione fatta e canale utilizzato. I dati sono inviati, al responsabile del *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* o al suo delegato.

Gli aggiornamenti avvengono in modo frequente e costante dalla rilevazione dell'incidente e per tutta la durata del disservizio. La durata del disservizio è intesa come il periodo di tempo in cui qualsiasi attività, processo o canale è o sarà probabilmente interrotto.

10.2. Classificazione dell'incidente

Se l'incidente registra un impatto tale da attivare potenzialmente uno degli scenari di continuità operativa preventivamente condivisi, il responsabile della *Business Continuity* (coinvolto nel Comitato di crisi di Flowe) attiva il *Business Continuity Office* di Banca Mediolanum per valutare, sulla base delle regole definite, la gravità dell'impatto dell'incidente e/o le azioni da adottare.

Il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* predispone per la seduta del Comitato di Crisi di Flowe, un documento con i dati utilizzati per formulare la proposta di classificazione dell'incidente ovvero:

- gli schemi forniti da *Business Strategy & Finance*, che hanno permesso di verificare il discostamento con i dati effettivamente lavorati;
- le considerazioni sull'effettivo impatto quali eventuali picchi di disservizio;
- eventuali azioni di contingency avviate;
- altri servizi a disposizione.

I referenti del *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* hanno l'onere di raccogliere e presentare tutte le informazioni raccolte sull'origine del disservizio, lo stato di avanzamento delle attività di risoluzione (se già avviate) o gli eventuali possibili interventi da attuare.

Il Comitato di Crisi, anche sulla base dell'istruttoria (dati forniti dai referenti e considerazioni raccolte), "delibera" la classificazione dell'incidente e l'eventuale segnalazione all'Autorità di Vigilanza, definendo i nominativi da inserire come referenti nella segnalazione, oltre alla data e all'ora della classificazione dell'incidente.

Si precisa che la classificazione deve avvenire entro 24 ore dalla rilevazione dell'incidente.

Nella stessa seduta viene inoltre definito se l'incidente determina l'avvio delle procedure di *Business Continuity* e se deve essere predisposta una comunicazione alla clientela impattata.

11. COINVOLGIMENTO DELLA CAPOGRUPPO

Il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence*, a valle della rilevazione di un incidente, 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 l'Ufficio Privacy di Banca Mediolanum (in caso di *data breach*) al fine di:

- condividere i dati e le informazioni relative l'evento rilevato e verificare le modalità/criteri con cui è stata formulata la proposta di classificazione (grave/non grave);
- discutere possibili impatti (es.: legali/reputazionali) sulla Capogruppo.

12. INOLTRO COMUNICAZIONE AGLI STAKEHOLDER

A fronte della decisione di procedere con la segnalazione all'Autorità di Vigilanza, il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* predispone, in collaborazione con tutte le unità organizzative coinvolte (*perspective*, Funzioni di Controllo), una bozza del rapporto iniziale al fine di permettere alla Capogruppo di inviarlo all'Autorità di Vigilanza entro le 2 ore successive all'avvenuta classificazione dell'incidente come "grave" da parte del Comitato di Crisi.

Si specifica che tale rapporto include le informazioni basilari dell'incidente, che rappresentano le caratteristiche fondamentali dell'incidente e le sue conseguenze, previste sulla base delle informazioni disponibili o in mancanza di questi, con le stime fornite da *Business Strategy & Finance*.

La bozza di rapporto viene condivisa dal *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* con l'*Unità di Supporto Manageriale Service Policy & Procedures* di Banca Mediolanum (per incidenti in ambito PSD2), con l'*Unità IT Security* di Banca Mediolanum (per incidenti in tema *cyber*) che si occupa dell'inoltro all'Autorità di Vigilanza attraverso le modalità e i canali preposti.

13. MONITORAGGIO RISOLUZIONE INCIDENTE

A seguito dell'inoltro del rapporto iniziale, il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence*, con il supporto del *Business Continuity Office* e delle *Perspective* coinvolte (in base al tipo di incidente), monitora lo stato di risoluzione dell'incidente e di ripristino dell'operatività.

Entro 3 giorni lavorativi dall'inoltro della prima segnalazione deve essere predisposto il report intermedio. Se l'anomalia si protrae nel tempo il *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* predispone una bozza di report intermedio ogni qual volta venga a conoscenza di cambiamenti significativi rispetto al rapporto precedente. Questo deve contenere una descrizione più dettagliata dell'incidente, il suo obiettivo è proprio quello di fornire un aggiornamento dello stato e delle conseguenze dell'incidente.

All'interno del report intermedio viene richiesta la compilazione delle seguenti sezioni:

1. informazioni generali, ulteriori rispetto a quelle richieste dal report iniziale;
2. descrizione dell'incidente, con una descrizione più dettagliata rispetto a quella richiesta dal report iniziale;
3. informazioni sull'incidente, secondo le tipologie già individuate nel format;
4. classificazione e impatto dell'incidente, con i criteri di classificazione interessati e i dati relativi all'impatto dell'incidente;
5. dettagli sull'impatto dell'incidente;
6. analisi, mitigazione e risoluzione dell'Incidente.

La bozza del report intermedio, una volta completato dal *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence*, viene condiviso con la *Funzione Compliance* - al fine di verificare la correttezza formale del modulo compilato - e *Risk Management*. A valle della condivisione viene inviato all'**Unità di Supporto Manageriale Service Policy & Procedures** di Banca Mediolanum (per incidenti in ambito PSD2) e l'**Unità IT Security** di Banca Mediolanum (per incidenti in tema *cyber*) che si occupa dell'inoltro all'Autorità di Vigilanza attraverso le modalità e i canali preposti.

Relativamente all'impatto reputazionale, si specifica che in un primo momento la valutazione su questo tema viene fatta dal Comitato di Crisi (sulla base delle considerazioni raccolte dalla *Funzione Risk Management*, dalla *Funzione Compliance*, dalla *Perspective Happiness & Service* e da *Business Strategy & Finance*).

Il report finale deve essere inoltrato entro 20 giorni lavorativi dalla risoluzione dell'incidente e ripristino dell'operatività, contiene la causa che ha originato l'incidente e la sintesi delle misure che sono state o saranno adottate per eliminare il problema ed evitare che si ripeta in futuro.

Il rapporto finale deve essere inviato una volta avviata l'analisi delle cause che hanno originato l'incidente (indipendentemente dal fatto che siano state già attuate misure di mitigazione o che sia stata individuata definitivamente la causa che ha originato l'incidente) e quando sono disponibili dati effettivi da sostituire alle eventuali stime effettuate.

Laddove si necessiti di una proroga del termine dei 20 giorni lavorativi (ad esempio, se non sono ancora disponibili dati effettivi sull'impatto) le Funzioni preposte della Capogruppo contattano l'Autorità di Vigilanza prima della scadenza del suddetto termine fornendo una giustificazione adeguata per il ritardo e una nuova data stimata per il rapporto finale. Nel caso il rapporto finale non includa tutte le informazioni necessarie perché non disponibili nei tempi richiesti (venti giorni lavorativi dalla chiusura dell'incidente), viene inviata una relazione di chiusura (nel formato standard del rapporto finale o libero, a seconda dei casi).

Le informazioni relative alla causa dell'incidente e alle misure adottate per evitare il ripetersi dello stesso sono fornite dal *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* che si avvale dell'aiuto della *Perspective Happiness & Services* in caso di errore operativo o nel caso in cui l'origine dell'incidente sia presso un fornitore esterno (Nexi/Temenos).

Se il problema è stato risolto entro i 3 giorni lavorativi successivi all'invio del report iniziale viene predisposto simultaneamente sia il report intermedio che quello finale nel medesimo report, ossia compilando le relative sezioni del modulo.

Si specifica inoltre che qualora nel Comitato di Crisi di Flowe sia stato definito di procedere con la comunicazione alla clientela, la *Perspective Happiness & Services* comunica al *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* i dettagli delle azioni di comunicazione intraprese al fine di riportarle nei report intermedio e finale.

14. ARCHIVIAZIONE DELLE INFORMAZIONI

Tutti i dati utilizzati dal *Team IT Operation, Security & Governance* della *Perspective Augmented Intelligence* a presidio e valutazione della tipologia di Incidente e degli impatti nonché i documenti prodotti per le eventuali segnalazioni all'Autorità di Vigilanza, sono archiviati a cura della stessa *Perspective* nello stesso registro di gestione degli *incident* realizzato con *Azure DevOps*.

Gli stessi vengono archiviati anche qualora il Comitato di Crisi di Flowe verifichi che non ci sono i presupposti per procedere con la Segnalazione all'Autorità di Vigilanza.

15. RIFERIMENTI NORMATIVI

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.

15.1. Normativa esterna

Si riportano di seguito i principali riferimenti normativi:

- *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";*
- *Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica, provvedimento della Banca d'Italia del 23 luglio 2019;*
- *Orientamenti in materia di segnalazione dei gravi incidenti ai sensi della Direttiva 2015/2366/UE (PSD2) EBA GL 2021/03;*
- *Istruzioni per la segnalazione dei gravi incidenti operativi o di sicurezza - significant institution italiane e banche autorizzate in italia appartenenti a significant institution straniera. - Banca d'Italia*


15.2. Normativa interna

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

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

16. ALLEGATI

Tutti gli allegati sono disponibili presso l'unità organizzativa owner della presente struttura.

ID	Descrizione allegato	File
1	Modello per la segnalazione di un grave incidente operativo o di sicurezza informatica - banche <i>significant</i>	 comunicazione_incidenti_SI_2021 (modulo).pdf